

Colorado Energy Assurance



Emergency Plan

The Colorado Energy Assurance Emergency Plan

June 2012

Supplement to the Emergency Support Function #12 (ESF #12 - Energy)

Annex to the State Emergency Operations Plan (SEOP)

State ESF #12 Co-Lead Agencies



Colorado
Energy Office



Dora
Department of Regulatory Agencies
Public Utilities Commission

Supporting Agency



Colorado Division of Emergency Management

Developed by
The Colorado Energy Assurance Advisory Group (EAAG)

Facilitated by
Center for International Security Policy Research, LLC (CISPR, LLC)

Table of Contents

Book 1 Table of Contents

I. Participants and Stakeholders	1
Introduction.....	1
II. Executive Summary	8
Book 1: Overview, Data Collection, and Future Progress.....	12
Book 2: Energy Assurance Action Plan.....	12
Book 3: Energy Sector Risk and Vulnerability Assessment.....	13
Book 3A: Hazard Typology and Quick Reference Guide - A Sub-Section of the Risk and Vulnerability Assessment, which serves as a stand-alone reference booklet.....	14
III Capabilities Gap Analysis.....	16
Introduction – Survey Results.....	16
Introduction – Workshops and Exercises	21
IV. Community Profile	33
General Information.....	33
Natural Resources	33
State EA Initiative.....	34
Legal Authorities: Developing a Legal Framework for Energy Assurance	36
Colorado Energy Office.....	38
Summary.....	42
V Plan Maintenance Process.....	43
Method and Schedule for Monitoring, Evaluating, Updating, or Revising the Plan.....	43
VI. Recommendations: Problem – Solution – Evaluation.....	45
VII. Conclusions.....	52

Book 2 Table of Contents

VIII. Energy Assurance Emergency Action Plan	1
Introduction.....	1
Response Strategy.....	2
Recovery/Restoration Strategy	24
Mitigation Strategy	44
Public Information Strategy.....	69

Book 3 Table of Contents

IX. Risk and Vulnerability Assessment	1
Assessing Existing Publications, Planning Mechanisms, Reports, and Studies.....	1
<i>Introduction</i>	<i>1</i>
<i>Renewable Energy Publications.....</i>	<i>1</i>
<i>Climate Related Initiatives</i>	<i>7</i>

<i>State and Regional Plans, Reports, and Studies</i>	8
<i>Risk Related Standards, Reports and Studies</i>	9
<i>Alignment with National and State Planning Mechanisms</i>	10
<i>State Framework for Emergency Management</i>	12
<i>Establishing the EA Communications Framework</i>	15
<i>Local Energy Assurance Plans</i>	18
Energy Sector Profile.....	20
<i>US and Colorado Electric Power Systems</i>	20
<i>Colorado Grid System Risks</i>	31
<i>Trends in the Industry</i>	32
Colorado Energy Resource Profiles.....	35
<i>Natural Gas</i>	35
<i>Renewable Resources</i>	44
<i>Coal</i>	55
<i>Hydroelectric</i>	60
<i>Liquid Fuels</i>	63
Smart Grid and Distributed Generation	70
<i>Smart Grid Considerations in the Colorado Energy Assurance Emergency Plan (CEAEP)</i>	70
<i>Distributed Generation Considerations in the Colorado Energy Assurance Emergency Plan</i> .	72
<i>Smart Grid and Distributed Generation Vulnerabilities</i>	74
Colorado Energy Sector Asset Database	77
<i>Costs and Strategic Approaches to Disruption</i>	80
<i>Understanding the Costs of Energy Disruption</i>	80
<i>Energy Sector Interdependencies</i>	85
<i>Interdependencies and Systemic Failures</i>	88
<i>Energy Infrastructure Interdependency Failures: Case Studies</i>	90
High Impact Low Probability (HILP) Events.....	97
<i>Cyberwarfare</i>	97
<i>Solar Weather</i>	132
Exercises	131
<i>Introduction</i>	131
<i>Organization</i>	131
<i>Intra/Inter-State Exercise: Cyber Attack</i>	132
<i>Inter-State Exercise: Geo Magnetic Storm</i>	143
<i>Western Region Energy Assurance Exercise</i>	151

Book 3A Table of Contents

X. Hazard Typology	1
Introduction.....	1
Definitions and Terms.....	2
<i>CEAEP Energy Sector Impact Score (ESIS)</i>	4
<i>Risk Composite Score (RCS)</i>	5
Natural Hazards	11
<i>Drought</i>	14
<i>Flood</i>	19

<i>Lightning</i>	24
<i>Tornadoes</i>	27
<i>Windstorms</i>	31
<i>Avalanche</i>	34
<i>Wildfire</i>	37
<i>Extreme Heat</i>	43
<i>Hailstorms</i>	44
<i>Precipitation</i>	47
<i>Thunderstorms</i>	48
<i>Winter Weather</i>	50
<i>Earthquake</i>	52
<i>Erosion and Deposition</i>	55
<i>Expansive Soils</i>	57
<i>Landslides/Mudflows/Rock falls</i>	60
<i>Landslides/Mudflows/Rock falls</i>	60
<i>Subsidence</i>	65
<i>Solar Weather/Geomagnetic Storm</i>	68
<i>Volcanic Activity</i>	70
Human-Caused Hazards.....	73
<i>Crime versus Terrorism:</i>	75
<i>Criminal Exploitation of Critical Infrastructure:</i>	77
Nuclear Attack.....	87
<i>Radiological Attack</i>	93
<i>Explosive Attack</i>	95
<i>Chemical Attack</i>	99
<i>Biological Attack</i>	104
<i>Physical Attack</i>	109
<i>Cyber Attack</i>	113
<i>Electromagnetic Pulse (EMP) Attack</i>	119
<i>Major Transportation Accident or Disruption</i>	122
<i>Dam failure</i>	128

References and Resources

Book 1: Overview, Data Collection and Future Progress.....	1
Book 2: Energy Assurance Action Plan.....	3
Book 3: Energy Assurance Risk and Vulnerability Assessment.....	4
Book 3A: Hazard Typology and Quick Reference GuideTM.....	13

Book 1

Overview, Data Collection, and Future Progress

Book 1 provides a comprehensive overview of the planning process and the current energy assurance situation in Colorado. It identifies gaps and objectives, provides a brief overview of the demographics and funding sources for energy assurance planning, and establishes guidelines for future plan maintenance. The book closes with an analysis of EA programs that may be suitable for implementation in the state of Colorado and provides a final conclusion of the benefits from Energy Assurance planning.

Book 1 Table of Contents

I. Participants and Stakeholders	1
Introduction.....	1
II. Executive Summary	8
Book 1: Overview, Data Collection, and Future Progress.....	12
Book 2: Energy Assurance Action Plan.....	12
Book 3: Energy Sector Risk and Vulnerability Assessment.....	13
Book 3A: Hazard Typology and Quick Reference Guide - A Sub-Section of the Risk and Vulnerability Assessment, which serves as a stand-alone reference booklet	14
III. Capabilities Gap Analysis.....	16
Introduction – Survey Results.....	16
Introduction - Workshops and Exercises	21
IV. Community Profile	33
General Information.....	33
Natural Resources	33
State EA Initiative.....	34
Legal Authorities: Developing a Legal Framework for Energy Assurance	36
Colorado Energy Office.....	38
Summary	42
V. Plan Maintenance Process	43
Method and Schedule for Monitoring, Evaluating, Updating, or Revising the Plan	43
VI. Recommendations: Problem – Solution – Evaluation.....	45
VII. Conclusions	52

The CEAEP is a comprehensive document that includes background information, reference materials, and other subject matter that may not be of interest to all readers. As a convenience, suggested sections are identified below for specific audiences.

For State Agencies and Local Emergency Management Stakeholders

- Executive Summary
- Capabilities Gap Analysis

For Energy Stakeholders

- Executive Summary
- Capabilities Gap Analysis

I. Participants and Stakeholders

(Presented alphabetically by organization under each heading)

Introduction

The Colorado Energy Assurance Emergency Plan (CEAEP) was developed through the leadership of the Colorado Energy Office (CEO), Public Utilities Commission (PUC), and the Division of Emergency Management (DEM) along with a strong alliance between Federal, State and local government agencies, public and private utilities, and private businesses. The participants and stakeholders, who have collaborated over the past two years, continue to be engaged and provide support in improving energy assurance throughout the Nation, Region, and State. An Energy Assurance Advisory Group (EAAG) was organized from the participants and stakeholders, which served as the subject matter experts (SMEs) during the Energy Assurance planning process. A special appreciation goes out to all stakeholders who worked diligently through the EA planning process so that the State of Colorado could provide its executive staff and the residents a meaningful Energy Assurance Emergency Plan. Participants and Stakeholders are listed alphabetically by organization under each heading.

LEAD AGENCY

Colorado Energy Office Angie Fyfe
 Douglas Karl
 Jonathan Miller
 Tom Hunt

PARTICIPATING STATE AGENCIES

Colorado Department of Regulatory Agencies – Public Utilities Commission
Director - Doug Dean
 Lawrence Duran

Colorado Division of Emergency Management (Listed by Sections)

Executive Staff: Director Dave Hard

Operations Section, Field Management:Randy Kennedy

Preparedness Section: Kerry Kimble
 Jason Finehout

Mitigation and Recovery Section:Marilyn Gally
 Victoria Smith

FEDERAL STAKEHOLDERS

Speakers - Workshop #3 – Cyber Security

National Institute of Standards and Technology..... Marianne Swanson
 U. S. Department of Energy..... Samara Moore

Exercise Participants

**Inter-State Exercise - Geomagnetic Storm Scenario
 Federal Emergency Management Agency (FEMA)**

Incident Management Assistance Team Andrew Batten
 Disaster Emergency Communications Roger Schroder

Inter-State Exercise and Western Region Energy Assurance Exercise

U. S. Department of Energy

Senior Technical Advisor/*Office of Electricity Delivery and Energy Reliability*..... Alice Lippert
 Project Manager - Energy Delivery Technologies Division..... Katherine Kweder

National Association of State Energy Officials Jeffrey Pillon

Critical Infrastructure Protection

U.S. Department of Homeland Security Joseph O’Keefe

REGIONAL STAKEHOLDERS

Michigan State University

Adjunct Associate Professor, Electrical and Computer Engineering Roger Koenig

STATE STAKEHOLDERS

Colorado Department of Consumer Counsel..... Jivaji More
 Jake Schlesinger
 Frank Shafer

Colorado Department of Labor and Employment

Division of Oil and Public Safety Mahesh Albuquerque

Colorado Department of Local Affairs

State Fleet..... Art Hale

Colorado Department of Public Health and Environment

Emergency Preparedness and Response Division Yonette Hintzen-Schmidt

Colorado Department of Public Safety(Listed by Divisions)

Division of Homeland Security Kevin Klein

Colorado State Patrol

Colorado Information and Analysis CenterMaj. Steve Garcia
 Homeland Security Section.....Cpt. J. P. Burt
 Office of Preparedness and Security..... Dr. Robin Koons

Colorado Division of Natural Resources
 Colorado Geological Survey Director Dr. Vince Mathews

LOCAL STAKEHOLDERS

City of Aurora
 Planning George Hoague
 Porter Ingram
 Howard Kaplan

City and County of Denver
 Utilities..... Kevin Magner
 Facilities..... Stephen Sholler
 Mayor’s Office of Emergency Management and Homeland Security.....Patricia Williams

General Services
 Data ManagementDawn Levin

City of Fort Collins
 Utilities Virginia Purvis
 Policy and Projects..... Tom Vosburg
 Information Security Quentin Antrim
 Health, Safety, and Security.....Wayne Sterler

City of Lakewood
 Environmental Services Division Brian Nielsen

City of Wheat Ridge
 Wheat Ridge..... Wade Hammond

Colorado Springs Utilities
 Business ContinuityTama Wagoner
 Information Technology Shannon Fair

PUBLIC/PRIVATE UTILITIES

Black Hills Corporation
 Regulatory Affairs Ann Hendrickson
 Reliability Center Alvin Pinkston
 Corporate Security Brian Ireland

Colorado Rural Electric Association Geoff Hier

Tri-State Generation and Transmission
 Corporate Security and Business Continuity Allan Wick
 Business Continuity and Chemical Security Dave Sayles

Xcel Energy, Inc.
 Enterprise Continuity Pete Judiscak
 Sr. Attorney Geraldine Kim
 Assistant Control Center Steven Owen
 Enterprise Continuity and Public Awareness Karen Rigggenbach-Vaughn
 Deb Watts

PRIVATE SECTOR

LEAP Contractors

AMEC Earth & Environmental, Inc Jeff Brislaw
 Hillary King

SAIC (R.W. Beck) Sabine Bendanoun
 Steve Brodsky

State EA GIS Contractor

Patrick Engineering, Inc Dave Updike

Private Business

Solarvolts, Inc Marvin Owens

EXERCISE PARTICIPANTS

Some stakeholders are cited more than once due to their participation in both workshops and exercises .

Intra-State Exercise – Cyber Attack

AMEC Earth and Environmental, Inc Jeff Brislaw
 Hilary King

Battelle Mike Spender

City of Aurora Matt Chapman
 Karen Hancock
 Porter Ingrum
 Marena Latch

City of Fort Collins	Wayne Sterler
City of Lakewood represented by EA Contractor SAIC	Sabine Bendanoun
Colorado Solar Volts.....	Marvin Owens
Colorado Springs Utilities.....	K. Kirshna Tama Wagoner
Colorado Division of Emergency Management	Kerry Kimble Jason Finehout
Colorado Department of Regulatory Agencies – Public Utilities Commission	Larry Duran
Colorado Energy Office	Matt Futch
Inter-State Exercise - Geomagnetic Storm	
AMEC Earth & Environmental, Inc	Hillary King
Black Hills Corporation	Ann Hendrickson Alvin Pinkston
City of Aurora.....	Porter Ingrum
City and County of Denver	Kevin Magner Patricia Williams
City of Wheat Ridge	Wade Hammond
Colorado Division of Emergency Management	Jason Finehout Kerry Kimble
Federal Emergency Management Agency (FEMA)	
Incident Management Assistance Team	Andrew Batten
Disaster Emergency Communications.....	Roger Schroder
Colorado Energy Office.....	Jonathan Miller
Michigan State University	
Adjunct Associate Professor, Electrical and Computer Engineering	Dr. Roger Koenig
National Oceanic Atmospheric Administration	
University Corporation for Atmospheric Research (UCAR).....	Director - Tom Bogdan
Space Weather Prediction Center (NOAA-SWPC).....	Executive Officer Dianne Suess
Branch Chief	Brent Gordon
Program Coordinator	William Murtagh
Tri-State Generation and Transmission Association, Inc	Dave Sayles

U. S. Department of Energy..... Katherine Kweder
Alice Lippert

Western Electric Coordinating CouncilKarl Fittinger

Xcel Energy Pete Judiscak
Steven Owen

Western Region Energy Assurance Exercise, Phoenix, AZ

Colorado Attendees

City and County of DenverPatricia Williams

City of Lakewood, EA Contractor SAIC Steve Brodsky
Brian Nielsen

City of Wheat Ridge Wade Hammond

City of Aurora and Wheat Ridge
represented by EA Contractor AMEC Earth & Environmental..... Jeff Brislawn

Colorado Division of Emergency Management (listed by rank) Kerry Kimble
Jason Finehout

Colorado Energy Office Jonathan Miller

Tri-State Generation and Transmission Association Allan Wick

**CENTER FOR INTERNATIONAL SECURITY POLICY RESEARCH, LLC (CISPR)
STATE EA CONTRACTOR**

EA Planning Team

Emergency Management and Energy Assurance PlannerProject Manager - Laura Nay

Exercise Coordinator and Assistant Project Manager Kent Smiley

Energy Economics and Policy Analyst..... Dr. Ed Sanders

Senior Smart Grid, Cyber Security & Critical Infrastructure Protection Analyst . Daniele Loffreda

State and Local Emergency Management Lead.....Judy Peratt

Research and Plans AnalystDr. Trina Rose

Quantitative Methods and Technical Editor PhD Candidate Mark Tallman

Graphics Design/Research Assistant Kathryn Tallman

Jr. Planner Lindsey Shafer

Interns – University of Denver Carla Hirashima
Amy Wong

II. Executive Summary

The Colorado Energy Assurance Emergency Plan (CEAEP) was developed to provide useful guidance and serve as a resource for the State of Colorado to improve emergency operations in preparing for, responding to and recovering from an energy sector power failure to include: electric power outage or disruption, natural gas delivery disruption, and/or liquid fuels shortage or delivery disruption. Here forward the CEAEP will be referred to as the “Plan.”

The State Energy Assurance (EA) Initiative, *“Enhancing State Government Energy Assurance Capabilities and Planning for Smart Grid Resiliency”* has been funded through the Department of Energy - Office of Electricity Delivery and Energy Reliability DOE(OE) and the American Reinvestment and Recovery Act of 2009 (ARRA). The Colorado Energy Office (CEO) as the award recipient has funded the project, building partnerships and exploring solutions to this comprehensive issue. Contributions that were provided by the core partnering State Agencies, in the development of the Plan, have brought a unique consortium to the table to accomplish the task.

- The Colorado Energy Office (CEO) – CEO promotes sustainable economic development in Colorado through advancing the State’s energy market and industry to create jobs, increase energy security, lower long-term consumer costs, and protect the environment. CEO has prioritized the Plan as a critical function for improving energy security throughout the State. As the lead agency on the project and the recipient of the DOE grant, CEO has been actively involved to ensure that the plan is complete, accurate and comprehensive. The office has collaborated with the partnering agencies, the Department of Regulatory Agencies – Public Utilities Commission and the Division of Emergency Management to help identify key components and interdependencies in the energy sector, serve a coordinating role for energy assurance exercises and manage the successful completion of the plan.
- The Department of Regulatory Agencies – Public Utilities Commission (DORA-PUC). The DORA-PUC serves a vital role as the regulatory agency for regulated utilities. Through the coordination of the PUC, the Department of Energy (DOE) and the National Institute of Standards and Technology (NIST) shared the most current data on cyber security and smart grid interoperability to Colorado’s utility stakeholders, who were critical components of the Energy Assurance planning process.
- The Division of Emergency Management (DEM) - DEM is responsible for the state's emergency management program which supports local and state agencies. Activities and services cover the five Phases of Emergency Management, which include: Prevention, Preparedness, Mitigation, Response, and Recovery for both natural disasters, such as flood, tornadoes, and wildfire, as well as technological and human-caused disasters such as hazardous materials incidents, and acts of terrorism.

Energy Assurance is collaboration between private and public entities with the common goal of exploring solutions for increasing energy reliability, resiliency and redundancy. Bringing together the appropriate private-sector players with interested Federal, State, local and regional

government stakeholders is the key to accomplishing a successful Energy Assurance Plan. In addition, the management of disaster operations when energy reliability is compromised requires unique consideration and involves distinctive sets of principles in response practices from private and public entities. Understanding the roles and responsibilities of each participating entity in advance of an outage or disruption is crucial to improved preparedness and streamlined operations that would restore an affected area to a pre-disaster status. Bringing together the vital players and harnessing the momentum throughout the EA planning process brought positive results and provided the impressive data presented in the Plan. The Colorado planning group is referred to as the Energy Assurance Advisory Group (EAAG) with representation from Federal, State and local government agencies, municipal utilities, private organizations, and major private-sector utility companies. The contribution and willingness to participate in this initiative by all went above and beyond expectations, but special mention is warranted for the involvement of the three major utility companies in Colorado and the Western Electric Coordinating Council, which continue to serve as the core members along with CEO, the PUC and DEM of the EAAG.

- Tri-State Generation and Transmission Association – Tri-State is a wholesale electric power supplier owned by the 44 electric cooperatives that it serves. Tri-State generates and transmits electricity to its member systems throughout a 200,000 square-mile service territory across Colorado, Nebraska, New Mexico and Wyoming. Tri-State provided two representatives throughout the EA planning process and attended the Western Region Energy Assurance Exercise in Phoenix. Their notable input from a generation and transmission perspective clarified their role and responsibility in relationship to the other utilities as well as their resource capability for power delivery in Colorado. Their expertise and knowledge of electric power infrastructure was invaluable in assessing capability gaps and developing potential initiatives for addressing those gaps. They remain engaged and supportive to continue with future EA planning efforts.
- Black Hills Corporation – Black Hills is a strong, diversified Investor Owned Utility (IOU) with operations that include Black Hills Power, Cheyenne Light Fuel & Power, and Black Hills Energy. These entities provide electric services to approximately 94,000 customers in southeastern Colorado and natural gas utility services to approximately 527,000 customers in Colorado, Iowa, Kansas and Nebraska. Black Hills Exploration & Production produces oil and natural gas in New Mexico, Wyoming and Colorado. Black Hills also has a fleet of power generation facilities in Colorado, Wyoming and South Dakota that produce more than 1,000 MW of energy annually. Throughout the EA planning process, Black Hills remained engaged providing unique and diversified information from a utility perspective. Their contribution played a role in clarifying processes to include: outage reporting requirements, restoration policy, investment incentives, the rate recovery process, and collaborative operational practices. Their leadership led to the development of an organizational EA communications framework and potential initiatives to share and track outage information.
- Xcel Energy – Xcel has regulated operations in eight Western and Midwestern states with revenue of more than \$10.3 billion annually. They own 300,000 miles of transmission and distribution lines and more than 35,000 miles of natural gas pipeline. Xcel services 3.4

million electricity customers and 1.9 million natural gas customers in eight states and is the larger provider in Colorado. Xcel Energy has been an instrumental Colorado partner with State and local government for many years. Their contribution to the EA process cannot be understated. Several Xcel representatives, each having a unique specialty, brought a variety of distinguished expertise to the planning table. During the Cyber Security workshop and exercise, they provided cyber and legal representation from their home office in Minneapolis. Their attendance and information sharing provided a clearer understanding of operational processes and better knowledge of the electric and natural gas infrastructure in Colorado. Their continued support has led to improved collaboration and liaison.

- Western Electric Coordinating Council – WECC is the Regional Entity responsible for coordinating and promoting bulk electric system reliability in the Western Interconnection. WECC is geographically the largest and most diverse of the eight Regional Entities that have Delegation Agreements with the North American Electric Reliability Corporation (NERC). WECC's service territory extends from Canada to Mexico. It includes the provinces of Alberta and British Columbia, the northern portion of Baja California, Mexico, and all or portions of the 14 Western states. WECC's participation came late in the EA planning process, but their contribution was crucial in making the connection and bringing the understanding of the industry's operational and reporting process to full circle. Their level of expertise and relationships with regulated and unregulated utilities brought collaboration between public and private enterprise to a new level. Their organizational structure and clearing house capability provides rapid access to outage information and potential resource mobilization in an electric crisis situation.

One of the most critical mechanisms for integrating energy assurance plan specifics is through the State Emergency Operations Plan (SEOP), administrated by DEM. It is a standard disaster operations structure used to manage state level disasters or emergencies. During SEOP activation, DEM brings appropriate *leads* from critical State Agencies, non-governmental organizations, and the private sector to the State Emergency Operations Center (SEOC) to assist DEM in managing support through mobilizing needed resources to the affected jurisdictions. These respective sectors are represented as an Emergency Support Function (ESF). Any one of these functions may have elements affected during a disaster that will be in need of resources to help manage the disaster. The SEOP categorizes these sectors as ESF #1 through #15 listed below:

Emergency Support Functions	
<p>ESF 1 – Transportation</p> <p>ESF 2 – Communications</p> <p>ESF 3 – Public Works and Engineering</p> <p>ESF 4 – Firefighting</p> <ul style="list-style-type: none"> • ESF 4a- Wildfire Suppression <p>ESF 5 – Emergency Management</p> <p>ESF 6 – Mass Care, Emergency Assistance, Housing and Human Services</p> <ul style="list-style-type: none"> • ESF 6a- Care of Companion Animals <p>ESF 7 – Resources Support</p>	<p>ESF 8 – Public Health and Medical Services</p> <ul style="list-style-type: none"> • ESF 8a- Behavioral Health <p>ESF 9 – Search and Rescue</p> <p>ESF 10 - Oil and Hazardous Materials Response</p> <p>ESF 11 – Agriculture and Natural Resources</p> <p>ESF 12 – Energy</p> <p>ESF 13 – Public Safety and Security</p> <p>ESF 14 – Long-Term Community Recovery</p> <p>ESF 15 – External Affairs</p>

Each ESF is represented by one or more State agencies. As an example, ESF #1 - Transportation would be represented by the Colorado Department of Transportation (CDOT), where ESF #11 - Agriculture and Natural Resources would be represented by the Colorado Department of Agriculture and the Department of Natural Resources. Long Term Community Recovery may be represented by many of the ESFs in planning for the comprehensive and long-term recovery of an impacted area.

ESF #12 - Energy is responsible for the collection, evaluation, and sharing of information on energy and power delivery systems damage, estimates on the impact of energy systems disruption and outages within affected areas, and estimates on restoration and recovery operations. The designated co-lead agencies for ESF #12 are the Colorado Energy Office and the Public Utilities Commission. Together they will provide expertise to assist DEM in gathering information from the affected energy sector. With that information, DEM can analyze the types of resources needed to mobilize in order to ensure the delivery of critical services as well as continuity of government operations throughout the duration of the incident.

“Energy Emergencies” include any level of power delivery system interruption, delay, or breakdown that affects the integrity of energy infrastructure and compromises continuity of life sustaining critical services to the public. The Plan, referred to as an “Emergency” Plan, suggests that its focus is primarily “*responding*” to an energy emergency. However, the unique structure of this Plan not only includes a response strategy, but also a recovery/restoration strategy, a mitigation strategy, and a public information strategy. Together and along with the Plans’ comprehensive risk and vulnerability assessment, it is designed with the intent, over time, to build reliability, resiliency and redundancy in the energy sector for improved power delivery sustainability. In order to highlight certain sections, the Plan has been organized in “Book” section, which is typically different from other State EA Plans. Book One combines elements of the EA planning process relative to the organization of the EAAG, data collection, and the future of EA planning and its processes. Book Two is the Energy Assurance Action Plan, which is a stand-alone book of strategies to respond to, recover from, and mitigate against energy emergencies. Book Three is the comprehensive Risk and Vulnerability Assessment of

Colorado's Energy Sector, which includes Book Three A, a Hazard Typology and risk probability methodology for the energy sector. The elements of each Book are identified below.

Book 1: Overview, Data Collection, and Future Progress

- **Participants and Stakeholders** – A comprehensive list of all participants and stakeholders.
- **Executive Summary** – An overview of the plan contents.
- **Capabilities Gap Analysis** – This section allows the reader to immediately understand the current Energy Assurance Picture in Colorado. The gaps were prioritized to formulate objectives and actions that when implemented would address “*where Colorado wants to be*” in terms of future Energy Assurance.
- **Community Profile** – This section includes some demographics, background on the funding source for Energy Assurance Planning, a legislative framework for both utilities professionals and emergency management practitioners, and a profile of Colorado's leadership in renewable energy development, conservation, and energy security.
- **Plan Maintenance** – This element details the process to ensure that the Plan will continue to be monitored, updated, and revised. It outlines tasks intended to harness the momentum this Plan has initiated and how it will continue to provide a framework for improved energy emergency operations and collaboration.
- **Recommendations** - The final recommendations suggest further exploration into programs most suitable for Colorado. Conducting benefit/cost analyses of such programs and investment feasibility studies are vital prior to implementation of any action. The programs listed were comprised from the examination of all data collected and consensus among the EAAG members to include building flexibility into the strategies for continued long term success.
- **Conclusion** – The conclusion highlights the significant elements taken from the EA Planning process and the importance of continued collaboration and attention for improving Energy Assurance.

Book 2: Energy Assurance Action Plan

- **Energy Assurance Action Plan** – The Action Plan is a compilation of three separate plan strategies and a public information component. They are designed to cover specific concerns of an energy outage or disruption relative to each phase of incident management. They were formulated based on the roles and responsibilities of energy stakeholders and the gaps identified. Together they establish a platform for streamlined communication and operation during the phases of an event. This platform allows for improved accuracy of information sharing among stakeholders and ensures information accuracy to the Governor. The Action Plan is designed as a lift-out section or “CD version on-the-go,” which can be used during an actual event. This enables easy access and ensures use of the Plan.
 - **Response Strategy** – Provides a platform for collaboration between public and private energy stakeholders for immediate response activities to an energy emergency.

- **Recovery and Restoration Strategy** – Provides a platform for collaboration between public and private energy stakeholders for recovery and restoration operations after the immediate imperative life-saving actions have been accomplished.
- **Mitigation Strategy** – Provides a platform for collaboration between public and private energy stakeholders for short and long-term mitigation measures as a recovery continuum to restore and reconstitute community to affected jurisdictions.
- **Public Information Strategy** – Provides a platform for collaboration between CEO, the PUC and DEM to disseminate accurate information to the public in coordination with DEM and the State’s Public Information Plan, which resides under ESF #15 – External Affairs.

Book 3: Energy Sector Risk and Vulnerability Assessment

- **Risk and Vulnerability Assessment** - Educates the reader about Colorado’s energy blueprint with a focus on the threats, risks and vulnerabilities to the overall energy sector, and the crucial importance of reliability on the electric sector from all other sectors of society.
 - **Assessment of Existing Planning Mechanisms** – This subsection starts off the Risk and Vulnerability Assessment section, with a comprehensive list and short summaries of the many plans, reports, studies, and documents reviewed during the EA Planning process.
 - **Energy Sector Profile**
 - U.S. and Colorado Electric Power Systems
 - Risks
 - Trends
 - Colorado Energy Resource Profiles
 - Natural Gas
 - Renewable Resources (Colorado’s Renewable Energy portfolio)
 - Coal
 - Hydroelectric
 - Liquid Fuels
 - Smart Grid and Distributed Generation – This sub-section covers the importance of Smart Grid technologies, their applications and increasingly new vulnerabilities; Distributed Generation programs; and understanding the internal relationship between these technologies
 - Colorado Energy Sector Asset and Database
 - Costs and Strategic Approaches to Disruption
 - **Energy Sector Interdependencies** - Expands on other aspects of vulnerability as it relates to interdependent networks. It provides an understanding for myriad impacts as a result of cascade failures among interdependent networks and the extent of dependency that critical sectors have on the continuity of operation of another sector and their vulnerability to cyber attack.
 - Interdependencies and Systemic Failure – This section gives special attention to the interdependent nature of the energy sector and all other sectors with regard to potential cascading systemic failures.

- Energy Infrastructure Interdependency Failure: Case Studies
- The Fukushima Daiichi Disaster
- **High Impact/Low Probability (HILP) Events** – Although HILP events are generally discussed in the Hazard Typology, this section gives special attention to two of the most feared hazards, one – a human caused hazard – Cyberwarfare, and two – a geophysical event - geomagnetic storm. It discusses the serious impacts that could be realized in a large scale event specifically the energy sector.
- **Exercises** – The dynamics of the exercises conducted throughout the EA process and the implications from the results are discussed in detail here as well as lessons learned from the Western Region EA Exercise orchestrated by DOE and NASEO. The Exercise Design Team decided that a cyber attack exercise and a geomagnetic storm scenario would be best to test capabilities in the energy sector of both the utilities and state and local government. The results added value to the content of the Action Plan Strategies.

Book 3A: Hazard Typology and Quick Reference Guide - A Sub-Section of the Risk and Vulnerability Assessment, which serves as a stand-alone reference booklet

- **Hazard Typology and Quick Reference Guide** – This comprehensive and very informative typology of both natural and human-caused hazards goes beyond a simple list of threats. Based on critical energy infrastructure assets and their relative risk and vulnerability to specific hazards, a rating scale and risk composite score ranking was developed to demonstrate general probability of impact to the energy sector from each hazard listed. The top seven natural hazards identified as priority threats by the EAAG are listed first as opposed to an alphabetical presentation; all others follow accordingly.
 - **Natural Hazards**
 - **Companion Natural Hazards Overlay Map Booklet** – Seven natural hazards were identified as the highest threat to energy sector assets. Patrick Engineering, Inc. was contracted to map the assets in each of the seven hazards zones by county and present the results in color in beautifully spiral-bound 11” x 17” booklets. This data is for official use only.
 - **Human-Caused Hazards**
- **References** – References are provided as a separate document for accurate cross-reference data used in the preparation of the CEAEP.
- **Appendices**
 - Planning Process
 - Energy Assurance Baseline Assessment
 - Legislative Framework
 - Exercises After Action Reports (AAR)
 - Current Affairs Articles
 - Renewable Energy Programs Case Studies

- Supporting Documentation
- Glossary of Terms

The Plan’s content allows for the reader to gain situational and historical awareness in order to respond efficiently to energy disruptions or emergencies. Throughout the Plan, graphics are used to help the reader visually understand the importance of the subject and where to obtain additional information.

III. Capabilities Gap Analysis

Introduction – Survey Results

Over the course of the EA planning process, data has been gathered to assess the energy assurance capabilities of the State of Colorado. This section focuses on key issues that are potential areas for improvement when responding to or recovering from an energy emergency and are presented at the beginning of the Plan to provide stakeholders with an understanding of the results of the data collected up front. Gaps are essentially the difference between “where we are” compared with “where we want to be.” In this case, the gaps identified were categorized by the level of capability the State of Colorado had, at the time of data collection, to respond to and recover from incidents of energy sector shortages, outages or disruptions. The term “State of Colorado” includes State government agencies and support agencies that would be involved in an actual incident of disruption at the State level, which indicates that local capabilities have been overwhelmed. The relationship between the State of Colorado and public and private energy sector utilities was critical in determining the current level of capability to respond to and recover from an energy emergency. Strategies were developed to address primary gaps and are located in the Energy Assurance Action Plan following this section.

Two techniques were used to identify the areas for improvement or gaps with Colorado’s energy assurance capabilities:

- **Questionnaire and Survey:** To obtain a baseline for comparison, a questionnaire was distributed to potential energy sector stakeholders in advance of the first regional workshop. Those surveyed included: State and local government agencies, public and private utilities professionals, public and private liquid fuels organizations, local emergency managers, first responders, and planners.
- **Exercises and Workshops:** A series of five workshops were facilitated to exchange information about the threats, risks and vulnerabilities facing the energy sector and to clarify roles and responsibilities between Federal, State and local government and private utilities or associated organizations. Each workshop had a specific focus to gather data in efforts to formulate the strategy of the Plan. An Exercise Design Team was identified to begin developing two exercise scenarios, a cyber attack on electric infrastructure and a significant geomagnetic storm. Colorado also participated in the Western Region Energy Assurance Exercise held in Phoenix, orchestrated by the Department of Energy (DOE) and the National Association of State Energy Officials (NASEO).

The following data is organized in chronological order from the beginning of the EA Initiative and as the topics were presented in the workshop sessions used during the EA planning process to gather data. Priority or severity of any one issue has not been established in this section other than the rating of answers received within the individual survey questions.

As the assessment continued and the Energy Assurance Advisory Group (EAAG) refined the results, potential solutions could be explored in attempts to close identified gaps and structure an improved EA strategy.

Initial Questionnaire/Survey Results

The questionnaire used to survey stakeholders contained two sections - general and specific. The general questions were related to threats, hazards, and associated risks relative to the energy sector emergencies and preparedness issues. The specific section questions focused on the level of knowledge the stakeholders had on cyber security, distributed generation, and smart grid technologies. The survey results were used as a baseline assessment of the current amount of in-house capability (understanding or knowledge of energy emergencies) across the state. One-hundred twenty-three questionnaires were emailed to government agencies, private entities, and associations that would be considered as stakeholders across the energy sectors including the electric, natural gas, and petroleum sectors. Only twenty-three responses were received – slightly less than 19% of those asked to participate. The representation of those who participated, however, covered electrical generation and transmission, liquid fuels exploration, storage and transport, state, county, and municipal offices of emergency management, state and local health and environmental, local law enforcement, public works, utilities, facilities, and data technology.

A sample of the main general questions section is presented here due to the length of the full questionnaire. The analysis of the results can be viewed in its entirety in the *Supporting Documents* section of the Plan appendices.

Surveyed Stakeholder's Representation

- 8 represent an Emergency Management Office: 2 State Level, 4 County Level, 2 Municipal Level
- 11 represent government agencies or offices other than Emergency Management:
 - 5 State Level
 - Public Health and Environment
 - Regional Public Health
 - Transportation
 - Oil and Gas
 - State Fleet
 - 6 Municipal
 - Public Works
 - Facilities
 - Data Analyst
 - Law Enforcement
 - Utilities
 - Health/Safety/Security
- 3 represent private sector utilities

- 1 represents private sector energy sales

A wide range of organization size was also represented.

- 14,000 staff/employees (large energy sector stakeholders)
- 3-5 employees (local OEMs)

Natural and Human-Caused Hazards

Below highlights the surveyed results and quantified a general prioritization for both natural and human-caused hazards. The percentage signifies how that portion of those surveyed responded.

Top Rated Natural Hazards	Top Rated Human-Caused Hazards
Tornadoes (77%)	Age of Infrastructure (70%)
Winter Weather (73%)	Inadequate Backup Supply (66%)
Fire/Wildfire (71%)	Major Transport Accident (64%)
Flood (57%)	Cyber Attack (57%)
Lightning (57%)	Equipment Failure (56%)
	Lack of Human Capital (51%)
	Radiological Hazard (50%)
	Supply Side Mgt. Disruption (50%)
	Chemical Hazard (46%)
	Demand Side Mgt. Disruption (36%)
	Railway Disruption (35%)

In-House Response and Recovery Capability

Percentages designate how those surveyed rated their own organizations’ in-house response and recovery capability as a “High Capability.” (Meaning adequately capable to respond to and recover from these types of hazards.)

Natural Hazards	Human-Caused Hazards
Flood (47%)	Equipment Failure (50%)
Winter Weather (43%)	Demand-Side Mgt. Disruption (40%)
Thunderstorms (43%)	Roadway Disruption (39%)
Fire (42%)	Transportation Accident (36%)
Earthquake (40%)	
Precipitation (40%)	

Number of People in Organizations with Expertise in EA Topics (0-5, 6-10, 11-15, 15+)

Table 1 indicates the number of personnel within the organization listed along the top that have expertise in the field listed along the left margin.

Table 1 Level of Expertise by Topic

	State EM	County EM	Local EM	State Oil/Gas	State Fleet	State PHE	Local Pub Wrks	Local Facilities	Local Data Mgt.	Tri-State	Black Hills
Smart Grid	0-5	0-5		0-5	0-5	0-5		0-5		0-5	15+
Distributed Generation	0-5	0-5		0-5	0-5	0-5		0-5		15+	11-15
Energy Supply Systems	0-5	0-5		6-10	0-5	0-5		0-5		15+	15+
Energy Assurance	0-5	0-5		0-5	0-5	0-5		0-5	0-5	0-5	15+
Emergency Response	0-5	0-5	15+	15+	0-5	15+	15+	0-5	0-5	15+	11-15
Damage Assessment	6-10	0-5	6-10	15+	0-5	15+		0-5	0-5	6-10	11-15
Emergency Restoration	6-10	0-5		0-5	0-5	15+	15+	0-5	0-5	15+	11-15
Emergency Recovery Operations	6-10	0-5	6-10	0-5	0-5	15+	15+	0-5	0-5	15+	11-15
Remote Control Facility	0-5	0-5		0-5	0-5	0-5	15+	0-5	0-5	15+	11-15
Pole Attachment Remedy	0-5	0-5		0-5	0-5	0-5		0-5		15+	11-15
Improved Guys/Anchors	0-5	0-5		0-5	0-5	0-5		0-5		15+	11-15
Cross-Arm Enhancement	0-5	0-5		0-5	0-5	0-5		0-5		15+	11-15
Weather Monitoring	0-5	0-5		0-5	0-5	6-10		0-5	0-5	0-5	11-15
Hot Spot ID	0-5	0-5		0-5	0-5	0-5		0-5		15+	11-15
Load Reduction	0-5	0-5		0-5	0-5	0-5		0-5	0-5	15+	11-15
Cyber Security Standards	0-5	0-5		0-5	0-5	6-10		0-5		15+	15+
Fuels Market		0-5		15+	0-5	0-5		0-5	0-5	15+	11-15
Fuels Supply		0-5		15+	0-5	0-5		0-5	0-5	15+	15+

Emergency Operations Centers

- 87% of respondents report that they have a dedicated EOC or similar facility

Policies, Memorandums of Understanding (MOUs), Intergovernmental Agreements (IGAs) concerning roles and responsibilities relative to energy emergencies

- 33% of those surveyed stated – Yes they have such documents

Performed a hazard analysis/risk assessment within last 5 years

- 72% of respondents have within last 5 years
- 50% have within last 3 years
- 75% have performed a risk assessment only within 3 years

Have developed an Emergency Operations Plan (EOP), Emergency Preparedness Plan (EPP), Continuity of Operations Plan (COOP), Continuity of Government Plan (COG), and/or Continuity of Business Plan (COB)

- 94% of the organizations surveyed have developed one of the above

Have participated in emergency response exercises

- 60% have participated

Knowledge of who to contact to build energy assurance

- 47% reported **not** knowing

Suggestions regarding coordination to improve redundancy/resiliency

- Ensure utilities are a part of an EOP, Emergency Support Function (ESF), and Emergency Operations Center (EOC)
- Include WestConnect or WECC in planning
- Educating each other on capabilities and how to assist one another
- Organizational chart with back-up individuals to build redundancy
- Agreement on communications process
- Common ground on identifying hazards and risks

Summary

The baseline survey outcome makes a general statement about the level of awareness concerning issues relative to energy emergencies. The compiled results provide a general perspective of concerns and issues related to energy emergencies. Thus, an appropriate approach for the EA planning process could be developed.

Introduction - Workshops and Exercises

The EA planning process was facilitated through a series of workshops and exercises that brought stakeholders together to better understand the threats, risks and vulnerabilities of the energy sector. A strategy was developed to improve response, recovery and mitigation activities for energy emergencies through identifying the gaps and better understanding of stakeholders' roles and responsibilities. This process helped advance momentum for potential solutions to build redundancy, resiliency and reliability within the energy sector with focus on electric power delivery.

Workshop #1 - Energy Assurance Plan and Advisory Group Kick-Off Meeting

The focus of Workshop #1 was securing the best audience for whom the information would be presented. A wide range of energy sector stakeholders and State agencies attended the first regional workshop. Information and data was presented on various threats, risks, and vulnerabilities within the energy sector. Emphasis on the interdependencies among sector-specific energy infrastructure was placed to stimulate discussion and preliminarily identify areas for improved collaboration between utilities professionals and emergency management practitioners. The primary purpose of Workshop #1 was to identify a core group of stakeholders that would participate throughout the EA planning process, which would make up the EAAG.

At the end of the presentations, stakeholders were divided into 3 groups:

- Table 1 - Emergency Management, Local Government and State Agency representatives
- Table 2 - Energy Professionals, Contractors, and Private Businesses
- Table 3 – Local Energy Assurance Plan (LEAP) Funded Municipalities, their Contractors and other associated energy businesses

The participants were asked to discuss among themselves the types of support needed from their counter-partners and other issues that impede operations during an energy emergency. The discussions were recorded with participant's permission to capture content. The following bullet points relative to gaps in processes were noted from those dictated discussions.

- Bring together utility professionals and emergency management practitioners to the same table to discuss opportunities to improve energy emergency disaster operations
- Identify an Energy Assurance Advisory Group (EAAG)
- Raise awareness about the risks and vulnerabilities facing energy-related critical infrastructure and key resources (CIKR).
- Identify gaps between professions
- Develop a platform for networking among all professions in the energy sector
- Identify Exercise Design Team
- Educate stakeholders with useful information about building energy assurance and recognizing the symptoms of potential disruption

The core EAAG that would remain constant through the EA Planning process included: CEO, the PUC, DEM, Tri-State Generation and Transmission Association, Xcel Energy, Black Hills Corporation, the City of Denver, City of Aurora, City of Wheat Ridge, City of Lakewood, and the City of Ft. Collins. Other crucial Federal, State, local and private stakeholders would be further identified bringing important information to the table as the EA planning process was refined.

Workshop #2 - Energy Assets Risk and Vulnerability Assessment – High Impact/Low Frequency Events

Detailed risks to the energy infrastructure and assets from the events of a geomagnetic storm (GMS) and cyber attack were further explored in Workshop #2, which highlighted unique vulnerabilities within the interdependent networks and their connectivity between energy specific sectors. The electric grid, Smart Grid (SG) technologies and Distributed Generation (DG) was discussed as potential mitigation strategies for building long term resiliency. Initial clarification of general roles and responsibilities were identified and a communications flow process to be used during an actual event was suggested. Preliminary Plan goals were generalized. The following areas needing improvement were cited.

General Areas

- More protection, education, and awareness about GMS
- Awareness training on cyber attacks and the impacts on energy sector interdependent networks
- Cyber Security Best Practices implementation
- Public Health component not included in cross sector exercise design
- Rural Hospitals rely on trauma centers for televised conferencing, if power outage they will be in severe crisis
- Develop working group for energy assurance issues
- Continued Smart Grid, Distributed Generation, and Microgrids research and development needed
- Improve collaboration with Emergency Management on
 - Medical registry
 - Curtailment Order
- Better identification of roles and responsibilities
- Better understanding of stakeholders’ operational processes
- Communities and individuals need more education on energy emergencies
- Safety education during electric emergencies
 - Safety for workers and community members
- Integration across the front – utility addressing customers, recovery partners communicating with EOCs, broader coordination
- Initial objectives for:

- Response
 - Improve communication and coordination between utilities and emergency management
 - Develop cooperative exercise activities
 - Work to develop a liaison strategy between utilities and emergency management
 - Clarify roles and develop an organizational hierarchy
 - Allocate resources
- Recovery
 - Develop damage assessment teams
 - Improve resource management/tracking
 - Maintain documentation of incident
 - Coordinate responsive agencies in recovery phase/mutual aid
 - Restore power
 - Initiate the Disaster Declaration process
 - Identify funding sources
- Mitigation
 - Improve monitoring for cyber attack
 - Raise awareness about solar weather hazards
 - Develop education programs about energy emergencies
 - Document lessons learned from historic events of energy disruption (electric, natural gas, liquid fuels, nuclear)
 - Improve threats and hazards identification to critical energy infrastructure
 - Conduct vulnerability analysis at the infrastructure/asset level
 - Evaluate age, weakened areas, potential infrastructure failure (research intensive)
 - Prioritize assets that need mitigation actions
 - Conduct Benefit/Cost Analysis
 - Harden most critical assets against most likely hazard(s)
 - Inventory resources (equipment and manpower)
 - Observe best practices in information sharing
 - Research funding opportunities applicable to implementing action items
 - Pursue planning opportunities
 - Continue implementation of Distributed Generation and Smart Grid applications
 - Maintain consistent public information message from utilities
 - Do not completely rely on the energy companies
 - Buy generators. Do not wait for the utility companies; help yourself.

Summary

The areas suggested for improvement above are further refined and categorized as the EA process continued.

Workshop #3 - Cyber Security

Since cyber attack and interoperability between specific energy sectors are considered a national priority, Workshop #3 was dedicated to presentations from the Department of Energy (DOE) and the National Institute of Standards and Technology (NIST) to educate and assist Colorado energy

stakeholders (primarily the electric energy sector) about standards and best practices developed by the industry leaders. An overview of NIST Interagency Report (IR) 7628 – Guidelines for Smart Grid Cyber Security along with NIST 1108 – Framework and Roadmap for Smart Grid Interoperability were presented by the Cyber Security Working Group (CSWG). These standards are provided as a model for improving cyber security and interoperability. The data presented would assist the EAAG in further identifying gaps in Colorado’s cyber protection practices and explore potential solutions to the issue.

Ongoing follow-up relative to cyber risk mitigation within the electric infrastructure included:

- Monitor cyber security and interoperability standards development from DOE , the Federal Energy Regulatory Commission (FERC) and NIST
- Track regulatory requirements to mitigate cyber threats initiated by FERC
- Follow legislation pertaining to cyber terrorism
- Recognition and implementation of cyber security best practices
- Establish and participate in Colorado cyber security working groups

Workshop #4 - Roles and Responsibilities, EA Emergency Functions and Hierarchy

Workshop #4 further clarified roles and responsibilities and explored potential outage tracking systems. Stakeholders left with a clearer understanding of outage reporting requirements and how sharing information on normal operational processes as well as processes during an event was vital in building relationships between professions. This helped to develop a coordinated public/private communication process for sharing electric outage information to streamline response and recovery operations. The EAAG agreed on four overarching goals for the plan.

- 1) Provide Public Welfare and Protect Critical Infrastructure
 - Notes: Life and Property Safety/Restoration of Lifelines
- 2) Improve Communication, Coordination, and Public Information
- 3) Expand and Improve Energy Assurance Awareness through Educational Outreach
 - Education/Preparedness
 - Improve outreach to public and EM community
 - Improve public awareness of energy issues and emergency alerts
 - Consider color codes
 - North American Energy Reliability Corporation (NERC) has guidelines for energy emergency alerts
- 4) Promote Public Policy to Improve Investment for Appropriate Reliability, Resiliency, and Redundant Systems

Combined Gaps Identified

- Clarify roles and responsibilities
- Inadequate knowledge about operational processes

- Disaster Declaration process
- What determines when a utility reports an outage
- Communication flow gaps about outages
- False perceptions about authority or lack of authority of State agencies
- Misunderstanding about purpose of CEO
- The need to understand the utilities’ operations and processes
 - Reporting outages specification
 - Prioritization of outage restoration
- Conceptualizing the need for an Energy Task Force (EAAG decided was not necessary for the energy sector as a task force would be for flood or wildfire)
- Gap in electric outage tracking processes (each utility has a different reporting requirement or lack of requirement)
- No convenient way for local or State officials to get outage information
 - Suggestion to utilize DEM’s WebEOC
- The need to expand data collection methods
- The need to streamline information sharing between utilities and local and State government
- Conservation requests from utilities to the public aren’t well received
 - Potential solution: ask the Governor to make the request instead of the utilities or media
- Recent exercise implies lack of communication between WECC/Utilities and EM community.
- Public information strategy needed
- The need to understand more about Natural Gas infrastructure and their interdependencies
- Inadequate Liquid Fuels Plan
- The stakeholders for petroleum and natural gas were absent (Xcel Energy provides natural gas)
- Utilities have MOUs for labor, not equipment – Is there a need for equipment MOUs?
- Building equipment redundancy
- Absence of a collaborative training or exercise program
- Insufficient supplies of appropriate tools, equipment, and manpower
- Insufficient educational programs to raise the level of awareness about energy emergencies
- The lack of understanding about useful existing tools that could be shared during outages

Workshop #5 – Energy Assurance Goals, Objectives and Action Items

The EAAG refined the overarching goals during Workshop #5. Potential objectives and implementable actions were also identified that address the Capability Gap Analysis. This process suggests a path to assist in achieving the overarching goals of the Plan. Some of the objectives and actions overlap all phases of an emergency (i.e., Prevention, Preparedness, Mitigation, Response, and Recovery) and some are specific to one phase. These objectives and action items are fully tabled in the Mitigation Strategy of the EA Action Plan and are noted with

an “x” in the proper column at the end of the objective or action, which designates which phase(s) it addresses.

The following are the Overarching Goals of the Plan

- 1) Provide Public Welfare and Protect Critical Infrastructure
- 2) Improve Communication, Coordination, and Public Information
- 3) Expand and Improve Energy Assurance Awareness through Educational Outreach
- 4) Improve Investment for Appropriate Reliability, and Resiliency

Intra-State, Inter-state, and regional Exercises - Gaps identified

(See Exercises – High Impact/Low Frequency Events section for full exercises details.)

Intra-State Exercise

Cyber Exercise

- **Gaps**
 - Lack of formal information sharing network between the utilities and State or Federal agencies
 - DEM does not receive reports on attacks or on current or potential outages
 - Lack of cyber attack reporting clearinghouse
- **Issues**
 - Reporting authority, if utilities are the victim of an attack, who should they report to?
 - Utilities implementing Smart Grid technologies collect and use significant amounts of customer usage data that could be used by criminal elements to track residential and business customer patterns. (i.e., resident behavior - at home, asleep, using computers, etc.)
 - Cyber security preventive measures in new projects are often left off the budget as they can prevent or delay the approval process or allow projects to meet marketing imposed implementation deadlines.
 - Phishing and human/social engineering attacks are more likely infiltration points than manufacturer introduced malware. This is especially true during a high stress or emergency situation when security protocols could be inadvertently relaxed or compromised to get back to business as usual.
 - Utilities are comfortable with sharing information with State and Federal regulators. However, they are not comfortable with that information getting into the hands of the media and public given the level of expectations for rapid speed of dissemination through social and media networks, and the ability to misunderstand or use the information - creating a bad public perception of the utility.

- What responsibilities do information security vendors have when they are trying to resolve issues with customers while simultaneously marketing their security products and expertise in resolving issues?

Inter-State Exercise

Geomagnetic Storm Exercise

• Gaps

- Large transformers restoration and replacement timeframe
 - 18 to 36 months
 - Transformer sharing capability
- Better understanding of network interdependencies and their impacts from GMS
- HF radio typically used by utilities as a secondary/backup communications system, not the primary system, so R-Scale (Radio Blackout hazard scale managed by NOAA) impacts to energy sector would probably not cause major impacts alone. Sectors that do rely heavily on HF-band communications are aviation and marine transport. Satellite communication can be disrupted, including GPS satellites. This could knock out service to PDA's and SatPhones/satellite TV/satellite internet. Combined with HF-band disruption, could significantly impact air and marine operations.
- Space Weather Prediction Center - Advanced Composition Explorer Spacecraft (SWPC: ACE Spacecraft) would be impacted by GMS event, would provide detailed input for subsequent alerts/warnings. Spacecraft is over 15 years old (well past its original service life). Spacecraft is fairly robust, but can be knocked out by extreme space weather. If this occurs, it is a severe event. It would prevent gathering detailed information for further solar hazards until brought back online.
 - The President has proposed funding for a replacement. Deep Space Climate Observatory may be launched by 2014.
- Geomagnetically Induced Current (GIC) causes extreme risk to energy/pipeline components. Damaging levels may or may not occur at the onset of a GMS event. It is more likely to suddenly spike without warning either minutes or hours into an event foiling precautionary or preventative measures.
- Do natural gas meter stations have backup power? Some do, some do not, but it's possible to restore pipelines manually, it's just more difficult and takes longer.
 - Often gas transmission pipelines are powered by gas, so they are self supporting
- In 1989, Quebec operators did not have ground current monitoring capabilities, couldn't respond in time.
- Even with ground current monitoring, sudden GMS spike could overwhelm mitigative measures. Areas at mid-latitudes (Colorado) may be particularly vulnerable because they typically do not have ground current monitoring.
- Liquid Fuels Issue: most utilities and many public and private entities use the same suppliers for diesel. An issue when everyone is on backup generators.

- Some healthcare facilities do not have backup power. Local EMs would attempt to address, and pass problems up the chain.
 - Most likely aged or non-acute facilities.
 - Hospitals usually have redundant systems
 - How often are they tested and/or checked?
- Replacement of transformers creates a number of issues.
 - Transformers are all manufactured overseas
 - Majority (if not all) of large capacity transformers are custom made
 - Demand will drive up prices
 - Foreign country competition
 - Delivery time is between 18-24 months in a non-event period. (Unknown if demand spikes)
- Space Weather prediction relies on satellite – Deep Space Climate Observatory. It is possible that a large storm will knock out the satellite and leave earth with little warning of storms occurring later for a number of years until a new satellite was deployed. Proposal, budget approval, build and launch will take at least 5 years.
- **Issues**
 - SWPC, WECC, and the utilities are cautious about issuing an alert of a G scale storm due to the ‘Cry Wolf’ scenario.
 - SWPC believes it has the tools to make a prediction
 - Consumer Protection? What about inspection of food at supermarkets/restaurants before returning to business? What about agriculture impacts?
 - Component Damage: There has been discussion about strategic component stockpiles. Most utilities keep spares, but certainly not for all transformers/components. Lead time to order new components typically as high as 18-24 months, only available from overseas vendors.
 - Purchase of spare components like large capacity transformers could cost as much as \$20 million per unit.
 - EEI does have voluntary spare transformer program.
 - Transformers are difficult to transport, and requires permits.
 - Stockpiled transformers also have significant costs just to keep them in storage and ready for use.
 - Tri-State: Does pre-stage some spare components, but not much.
- **Discussion**
 - SWPC: Suggests assessment of supply chain vulnerabilities.
 - NERC reports on the subject have been "dire."
 - If utilities turn off their transformers, causing widespread blackouts, to protect their equipment, an outage of 4-8 hours will have little impact on communications or other emergency backup power systems. Once the outage extends to 12 hours and beyond, such localized power redundancy becomes impacted.

Regional Exercise

Western Region Energy Assurance Exercise sponsored by – U.S. Department of Energy (Phoenix, AZ)

- **Gaps**
 - More focus on petroleum and building relationships
 - Regional Collaboration
 - Building regional relationships
 - Regional exercises
 - Outreach to different groups and associations
 - Cyber Security working group/clearinghouse
 - Back-up power generation capacity
- **Scenarios**
 - A 9.0 magnitude “Cascadia” earthquake and resulting tsunami
 - Cyber attacks to the petroleum and natural gas infrastructures with cascading impacts on the electric infrastructure in the Western region
 - Truckers’ strike impacting petroleum supplies

Evaluations

Participants were numbered off and grouped so that each participating State and/or Territory was represented in each breakout room as thoroughly as possible. Discussions were to take place on each scenario to evaluate how the scenarios would impact their State, Territory, cities, counties, and the overall region.

- **Issues Highlighted**
 - How would State and local government and industry evaluate the emergency event and its impacts?
 - How would preliminary assessments of the magnitude and duration of the emergency be developed?
 - What response measures would participants take in the event of such an emergency?
 - What interdependencies pose the greatest concern and why?
 - In their energy assurance plans, have States and localities considered impacts similar to those from the scenarios?
 - What lessons have State and local participants learned as a result of these emergency scenarios, and what actions may they take within their organizations to improve their energy assurance?

Colorado Impacts - Scenario #1 – Cascadia Tsunami

Although Colorado was not directly impacted by the tsunami itself, cascading secondary impacts were realized.

- The State Emergency Operations Center would be activated to respond to Emergency Management Assistance Compact (EMAC) requests and assist in systematic deployment of resources to the Pacific Northwest impacted region.
- Regional Balancing Authorities would coordinate with their Northwest counter-partner to assist in assessment, restoration and recovery operations depending on establishing a priority restoration process.
- The Colorado Energy Office (CEO) along with the DORA – Public Utilities Commission would serve as an ESF #12 Co-Lead Agency to coordinate with DEM for assistance.
- Other infrastructure systems impacts and needed resources would be handled through the appropriate ESF at the SEOC.
- Colorado would/could experience impacts at all levels affecting the economic structure of the State for an extended timeframe.
 - Petroleum delivery disruption (much of the liquid fuels resources would/could go to the Northwest for recovery operations)
 - Inflation on products and produce from the Northeast
 - Costs of resource mobilization (should CO deploy resources)
 - Impacted banking and finance networks, circulation of money
 - Cyber networks vulnerability and rerouting necessities

Scenario #2 – Cyber Attack: 42 million people without power

Colorado would be severely affected by the magnitude of this scenario. With the volatility of power restoration, critical life-saving facilities would have to rely on back-up power generation. A good analysis of which entities are backed-up doesn't really exist from a state level. Individual municipal and county government operations may have a better perspective on what is backed-up in their area. Larger medical-related service facilities have back up power generation, but smaller ones do not. Critical measures would have to be activated immediately if the entire state was expected to be powerless even for more than a few minutes. Each municipality, county and State level operations would be activated to ensure that public safety was protected resources could be deployed accordingly.

- **Heaviest impacts (not in priority of severity)**
 - Liquid Fuels operations, pumping capabilities failure
 - Electric and Natural Gas power delivery failures
 - Critical government and life-saving services
 - Adequate fuel for all back-up generation
 - Feeding and Sheltering operations to accommodate “all” special needs populations
 - In-Home critical health needs response operations
 - Food and agriculture refrigeration and operations capabilities
 - Public Health and Environment laboratory facilities impact
 - Information Technology services within government facilities
 - Public Information processes for keeping the affected public informed
 - Water/Waste Water systems

- Water pumping stations
 - Waste Water systems processes
 - Banking and financial networks failure
 - Financial transactions incapability
 - Money circulation issues
 - Credit card processing
 - Transportation systems operations (traffic lights, light rail, bus systems, railway transportation, air travel – Denver International Airport)
 - Transportation of fuels, rescue operations, recovery operations severely hampered
 - Public Information and media access failure
 - Economic impact (business operations failure)
 - Military installations operations
- **Impact Assessment and Recovery Operations of the cyber network**
 - Cyber security investigation and assessment going on behind the scenes (at each entity and at a regional level) to quickly solve the point of failure(s)
 - Recovery may be a patch-work process on many fronts to temporarily get operations back up and running, then a more intensified evaluation of what it will take to fix the cascading problems will ensue.
 - Cyber Working Groups will organize and evaluate at the larger impact perspective

Scenario #3 – Independent Trucker Strike

Colorado would certainly be affected if an Independent Trucker Strike were to occur and continue for any length of time. There are several large truck stops throughout Colorado, but particularly concentrated in the Denver Metro area. Colorado's attendee from the City of Wheat Ridge Police Department stated that Travel Center of America Truck Stop in Wheat Ridge was the largest one in the Denver area. His city would be greatly impacted by a trucker strike.

- **Local Considerations**
 - Increased police protection in case of a civil disruption
 - Pre-staging in preparation for civil disturbance
 - Ask for State and other jurisdiction Law Enforcement back up manpower
 - Assessment of fuel availability for government fleet, law enforcement, fire and EMS operations
 - Preparedness to provide for lack of delivery of produce, water, baby formula, dairy, and meat items to local grocers
 - Public/Private negotiations between city and fueling stations to assess fuel allocation consideration for public use
- **State Considerations**
 - State Fleet fuel reserves assessment
 - Monitoring for State resources should civil disturbance occur

- Early negotiations between State Colorado Energy Office and fuel supply/markets
- CEO potential to act as a mediator between truckers and fuel supply (if that is possible for temporary reduction in diesel fuel costs to alleviate situation)
- Review transportation fuels policy, practices, programs and establish early relationships with appropriate contacts
- **Lessons Learned from Western Region Energy Assurance Exercise**
 - Liquid Fuels is a key component to EAP
 - CEO plans to hire a Transportation Fuels Specialist upon return from exercise and update Liquid Fuels Plan (This was accomplished as of January, 2012)
 - State level planning with other States and regions
 - Utilize resources like the Western Governors Association
 - State level Cyber Security. Realization that it is a global concern
 - Cyber Security Working Groups should be established if not already done so.
 - Include cyber security personnel in exercises and planning functions
 - Monitor Federal guidelines for cyber security in electric utilities (PUC currently has this responsibility)
 - Advocate that utilities have in place securities at least at the level of Federal guidelines
 - Be prepared at the State level (PUC) to establish cyber security guidelines should it be placed within the State’s authority to monitor/regulate (The PUC will advocate and support DHS, DOE, FERC, NERC established guidelines in order for there to be consistent industry-wide cyber security risk mitigation)
 - Continue to clarify roles and responsibilities between the stakeholders during an energy emergency to streamline response and recovery activities
 - Continue planning sessions with the Energy Assurance Advisory Group at least on a quarterly basis
 - Use ISERnet and other official sites for monitoring Energy Assurance information

Summary

The Capabilities Gap Analysis includes all areas considered potential for needing improvement. The EAAG identified a variety of possible solutions to address the gaps. The terms “Potential Initiatives” and “Potential Action Items” are used to address the gaps and are categorized under the appropriate

The Overarching Goals of the Plan are presented in **Table II-1 Goals, Potential Initiatives, and Action Items** at the end of the Mitigation Strategy.

IV. Community Profile

General Information

Colorado, the Centennial State, was admitted into the Union as the 38th state in 1876. It encompasses most of the Southern Rocky Mountains as well as the northeastern portion of the Colorado Plateau and the western edge of the Great Plains. It is part of the Western United States, the Southwestern United States, and the Mountain States. Its land mass is 8th and its population is 22nd out of the 50 United States. Colorado is noted for its vivid landscape of mountains, forests, high plains, mesas, canyons, plateaus, rivers, and desert lands. Its climate is complex where extreme weather can be a common occurrence due to its geological variance.

The United States Census Bureau estimates the population at 5,116,796 in 2011, which is an increase of near 2% since 2010. The Denver metropolitan, which includes Denver-Aurora-Boulder Combined Statistical Area had an estimated population of 3,110,436 in 2009 and is home to 61.90% of the state's residents. The state's fastest-growing counties are Weld and Douglas, which are at the extreme north and south end of the Front Range Urban Corridor. By 2020, estimates of near a million new residents will inhabit Colorado's Front Range.

Colorado's economy was ranked 11th in the nation in 2010. Its central location and geological diversity makes it an attractive hub for a variety of national and international businesses. The federal government is also a major economic force in the state, housing many vital facilities to include: the North American Aerospace Defense Command (NORAD), United States Air Force Academy, Schriever and Peterson Air Force Base and Fort Carson United States Army installation, all of which are located south of Denver in the Colorado Springs area. The National Oceanic and Atmospheric Administration (NOAA) and the National Institute of Standards and Technology reside in Boulder and the Renewable Energy Laboratory (NREL) has its campus in Golden. The U.S. Geological Survey, the Federal Emergency Management Agency (FEMA) Region VIII, and other government agencies are located at the Denver Federal Center in the City of Lakewood west of Denver. The Denver Mint and 10th Circuit Court of Appeals are located in the City of Denver with Buckley Air Force Base east of Aurora. The United States Penitentiary, Administrative Maximum Facility (ADX) is a federal *Supermax* prison located near Cañon City employing near 400 residents. In addition to these and other federal agencies, Colorado has abundant National Forest land and four National Parks that contribute to the federal ownership of 24,615,788 acres or 37% of the total area of the state. In the second half of the 20th century, the industrial and service sectors have expanded greatly. The state's economy is diversified and is notable for its concentration of scientific research and high-technology industries.

Natural Resources

Colorado has significant hydrocarbon resources. According to the Energy Information Administration (EIA), Colorado hosts seven of the Nation's 100 largest natural gas fields and two of its 100 largest oil fields. Conventional and unconventional natural gas output from several Colorado basins typically account for more than 5 percent of annual U.S. natural gas

production. Colorado’s oil shale deposits hold an estimated 1 trillion barrels of oil – nearly as much oil as the entire world’s proven oil reserves. The economic viability of the oil shale has not yet been demonstrated though continues to be an economic focus for development. Substantial deposits of bituminous, sub-bituminous, and lignite coal are also found in the state as well as Kimberlite volcanic pipes, which produce quality diamonds. Colorado's high Rocky Mountain ridges and eastern plains offer the perfect landscape for the development of a renewable energy portfolio. Wind, solar, hydro and geothermal activity for power generation is under way in areas across the state along with ethanol production in Northeast Colorado. Detailed profiles are discussed later in the Plan.

Considering Colorado’s potential for robust renewable energy source development and its continued population growth, it is imperative to plan and manage the supply and demand for electric and natural gas power generation, transmission and distribution. The opportunity to explore and improve energy assurance with funding from the Department of Energy was timely and appropriate for interested energy stakeholders in Colorado.

State EA Initiative

“Enhancing State Government Energy Assurance Capabilities and Planning for Smart Grid Resiliency”

The funding opportunity allocated to the State of Colorado for this initiative was made possible through the Department of Energy: Office of Electricity Delivery and Energy Reliability (OE) and the American Reinvestment and Recovery Act of 2009 (ARRA) and awarded to the Colorado Energy Office.

The goal of the American Recovery and Reinvestment Act of 2009 is to make supplemental appropriations for job preservation and creation, infrastructure investment, energy efficiency and science, assistance to the unemployed and State and local fiscal stabilization. The main focus of this initiative is to “facilitate recovery from disruptions to the energy supply” and “enhance reliability and quicker repair of outages” and in doing so create jobs, which stimulates the economy. The State EA Initiative allows the State of Colorado to have well-developed, standardized energy assurance and resiliency plans that will serve as a basic decision-making tool during energy emergencies and supply disruptions. This initiative also allows the State to address energy supply disruption *risks and vulnerabilities* to lessen devastating impact that such incidents have on the economy and the health and safety of citizens. It also focuses on developing new, or refining existing, plans to integrate new energy portfolios (renewables, biofuels, etc.) and new applications, such as Smart Grid technology, into energy assurance and emergency preparedness plans. Better planning efforts will help contribute to the resiliency of the energy sector, including the electricity grid, by focusing on the entire energy supply system, which includes generation, transmission and distribution of power and refining, storage, and distribution of fossil and renewable fuels. The National Association of State Energy Officials (NASEO), with the Department of Energy has prepared the State Energy Assurance Guidelines (<http://www.naseo.org/eaguidelines/>) which served as a model for the development of the Plan

along with other Federal and State planning guidelines, to include, the National Response Framework, the Federal Emergency Management Agency State and Local Mitigation Planning “How To” series; the Comprehensive Preparedness Guide (CPG 101) version 2.0 September 2010 – Developing and Maintaining Emergency Operations Plans; and The Colorado Homeland Security Strategy 2008-2013.

Benefits

The benefits of the State EA Initiative are many. Creating the current Plan and understanding new energy portfolios will assist in the endeavor to build resiliency, reliability, and redundancy; however, it is the continued collaboration and coordination among stakeholders that will deliver the practicality of its contents. The benefits include:

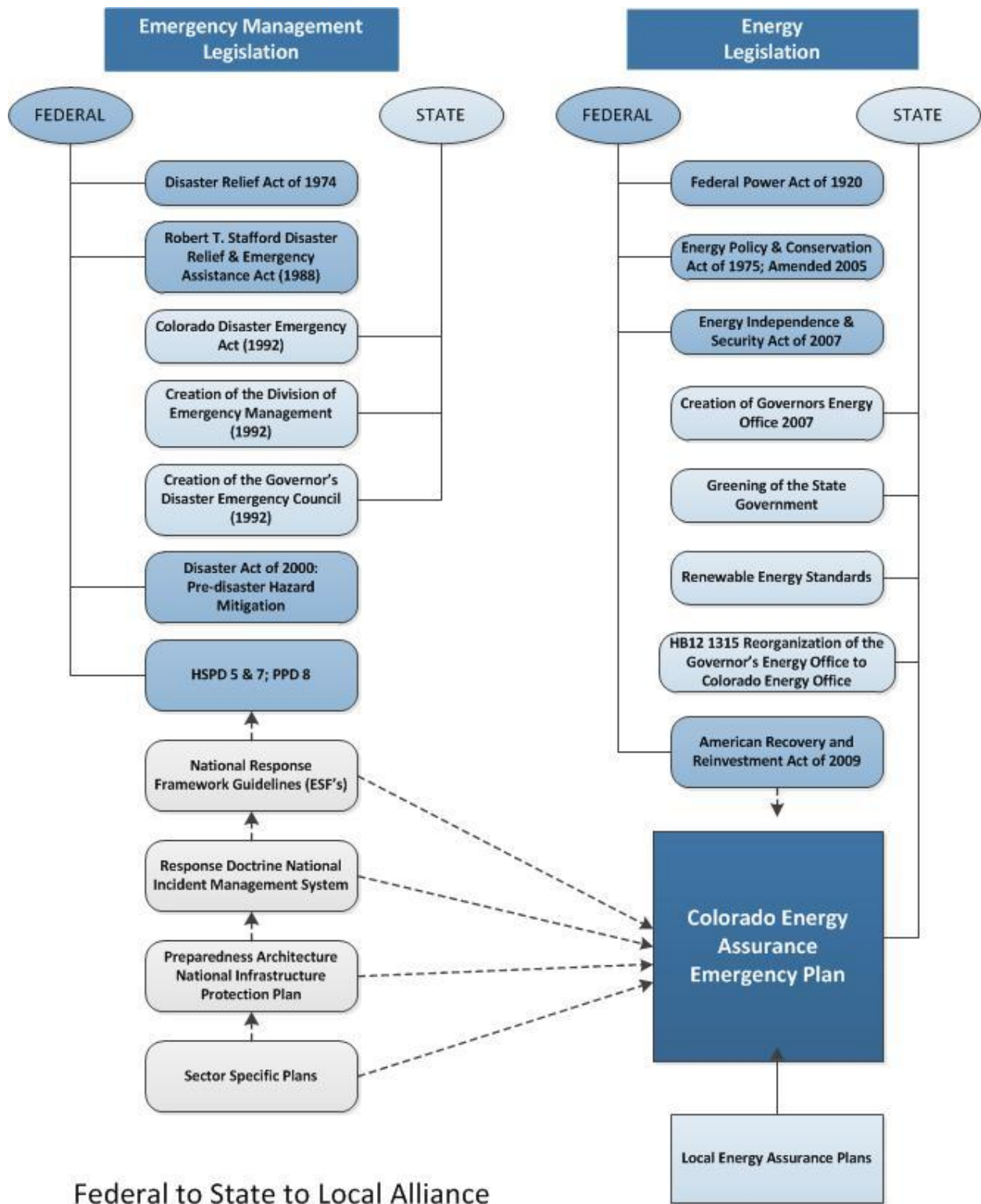
- The organization of an Energy Assurance Advisory Group (EAAG) early in the process to analyze the problems, concerns and issues surrounding energy emergencies and bridge the gap between Utilities Professionals and Emergency Management Practitioners relative to energy emergencies operations.
- Creating in-house expertise at the State and local government level about energy assurance planning and what building redundancy can accomplish. Its reference here is to cross-train, educate, and designate a second tier of equally knowledgeable expertise about energy assurance into the daily regimen of operations.
- Building redundancy into the power delivery systems, is the same concept, but applied to equipment resources. This type of redundancy can assure a back-up power generation capability for critical services, such as liquid fuels power generators and much more.
- Coordination in building regional reliability through two tabletop exercises, an **Intra-State** and an **Inter-State** exercise and the opportunity to participate in **Regional** Energy Assurance exercises orchestrated by DOE and NASEO. The exercises provide an opportunity to test in-house capability as well as regional collaboration. Capability gaps identified assist in the development of potential implementable actions intended to build a stronger state to regional response and recovery strategy.
- Identifying Overarching Plan Goals through the EAAG where members are in support of the State’s vision for energy assurance. *Potential Initiatives* as well as *Potential Action Items* outlined are structured for response, recovery and mitigation strategies in efforts to achieve the overarching goals. This strategy encompasses the complexity of managing an energy emergency from onset to restoration to future protection.
- Further defining the complexities involved in the interdependencies between power delivery systems and sectors; and be cognizant of the potential for cascading vulnerabilities. In doing so, programs can be identified to better protect energy infrastructure assets.
- Tracking and monitoring energy emergencies where quantitative data can be gathered on the severity of an event and used for improving future preparedness or mitigation strategies. It is the goal of this initiative to improve strategies that reduce impact costs and pursue the exploitation of Smart Grid and Distributed Generation technologies where application could increase security, resiliency, and emergency outage management.

Legal Authorities: Developing a Legal Framework for Energy Assurance

Introduction

Planning for energy assurance necessitates the understanding of laws and directives pertaining to both, power delivery systems and the practices of emergency management. Legal research was conducted to identify critical milestones in the legislative processes for both industries. A comprehensive reference document was developed; however, due to its length is not included here. It can be viewed in full in the References section. The visual representation in Figure 1 is an organizational display of select legislation pertinent to disaster management and the energy sector that provides a simplified pattern of legislative progression. Together they build a platform from which energy stakeholders and emergency management practitioners can successfully collaborate and address energy assurance issues to improve reliability and resiliency.

Figure 1 Legislative Organizational Chart



Colorado Energy Office

2012 Legislative Session - House Bill 1315

The Colorado Energy Office was introduced through HB1315 in the 2012 legislative session. Key elements of the bill included:

- Changes name of the office to “*Colorado Energy Office*” (Previously the Governor’s Energy Office).
- Secures continuous funding for the Office for 5 years.
- Established two funds:
 - **Innovative Energy Fund:** can be used for promoting, research, development, commercialization, education, attracting innovative industry investments to the state, providing market incentives for efficient innovative energy products, assisting in implementation of innovative efficiency projects, aid government agencies in innovative energy efficiency initiatives, and innovative energy policy development. Innovative energy is defined as “existing, new, or emerging technology that enables the use of a local fuel source, establishes a more efficient or environmentally beneficial use of energy & helps to create energy independence & security for the state”. The funding source is derived from severance tax dollars.
 - **Clean & Renewable Energy Fund:** can be used for attracting renewable energy industry investment in the state, assisting technology transfer into the market place for newly developed energy efficiency and renewable energy technologies, providing market incentives for the purchase & distribution of energy efficient & renewable energy products, assisting in energy implementation of energy efficiency projects throughout the state, aid government agencies in energy efficiency initiatives, implementation of renewable energy technologies, overall advancement of energy efficiency & renewable energy throughout the state. The funding is derived from General Fund dollars.
- Requires the Colorado Energy Office to report to the Legislature annually via the SMART Act.

Notable History

John Hickenlooper Administration

In January 2011, Governor John Hickenlooper was inaugurated with the vow to promote sustainable economic development in Colorado through advancing the State’s energy market and industry to create jobs, increase energy security, lower long-term consumer costs, and protect the environment.

Mission Statement: To promote sustainable economic development in Colorado through advancing the State's energy market and industry to create jobs, increase energy security, lower long-term consumer costs, and protect our environment.

- **2011-2012 High-Level Goals**

- **Conduct a stakeholder engagement process** to evaluate the costs and benefits of Colorado's electric power sector and work to develop an energy portfolio that promotes sustainable economic development.
 - Establish a stakeholder process with participation from the electric power utilities, universities, consumer representatives, environmental groups, State and Federal Agencies, and fuel sector industries.
 - Deliver a consensus-based report on the analyses and policy recommendations to the Governor by May 31st, 2012.
- **Increase the adoption of compressed natural gas (CNG)** as a component of a balanced energy portfolio for transportation fuels, by:
 - Signing an MOU to aggregate demand from local, state, and Federal fleets for annual purchases of CNG-capable vehicles from fleet owners in order to establish bulk order necessary to stimulate production by OEMs at an incremental cost less than \$7000 per vehicle by June 1st, 2012.
 - Develop and demonstrate a business case by June 30, 2012 for natural gas vehicles through three commercial-scale pilots in distinct vehicle segments throughout Colorado. Through these pilots, CEO will seek to identify and mitigate market barriers and quantify benefits to Colorado, which will be summarized in a case study to be distributed to organizations including, but not limited to: the Colorado Municipal League, Colorado Counties, Inc., Colorado Association of School Boards, Special Districts Association of Colorado, Colorado Natural Gas Vehicles Coalition, Colorado Association of Transit Agencies, Colorado Oil and Gas Association, Colorado-Wyoming Petroleum Marketers Association, and Clean Cities.
- Eliminating the roadblocks to residential and commercial energy efficiency financing by overcoming the existing market barriers through:
 - Identifying the preferred method for ensuring energy efficiency improvements are valued in the residential market by working with local banks, utilities, and appraiser groups to issue a consensus-based market advisory document for Colorado energy efficiency financing by January 31st, 2012.
 - Work with the Colorado appraisal community to issue an agreement in principal to develop a standardized process for credibly evaluating, valuing, and documenting the energy performance of single family housing units by March 1st, 2012,
- Support the administration's efforts to **boost the innovation ecosystem** in the State of Colorado by:
 - Conducting and publishing a report analyzing the innovation ecosystem in the State's energy sector, identifying the strengths and weaknesses, analyzing the gaps, and developing a plan for evaluating the State's role by April 1st, 2012.
 - Administering the CEO Revolving Loan Fund, including

- Closing \$7 million in additional loans by December 1st, 2011
- Restructuring the program to increase the capital leverage for the use of funds returned to the program through repayment by May 1st, 2012.
- **Increase the energy literacy** in the State of Colorado to ensure informed and productive conversation on energy choices by the public, opinion-makers, business sector, elected representatives, and appointed officials, including:
 - Spinning out the RechargeColorado website and rebate program to create a third party, not-for-profit run, source of retail energy information by April 1st, 2012.
 - Launching a new CEO website, which will provide easy access to the data from reports, such as, the CEO STAR report, jobs and investments studies, information about implicit and explicit costs, and project information, for CEO programs by November 1st, 2011
 - Developing and implementing a strategic plan to survey, evaluate, and address knowledge gaps across segments of the Colorado population by February 1st, 2012.

Bill Ritter Jr. Administration

The Governor's Energy Office (GEO) was created in 1977 with the purpose of promoting energy conservation in Colorado under the original name of Governor's Office of Energy Management and Conservation. Incoming Governor Bill Ritter, Jr., in 2007, knew that advancing energy solutions would be a priority for Colorado. By April 2007, he established the Governor's Energy Office to advance and manage his Blueprint for doing so. The Colorado Renewable Energy Collaboratory was created by US Senator Ken Salazar as a partnership tying the National Renewable Energy Laboratory (NREL) to Colorado's three major research universities: the University of Colorado, Colorado State University, and the Colorado School of Mines. Together they would train the "next-generation" scientists and engineers for renewable research and development. The Governor's Energy Office provided management for a variety of energy programs and administration of millions of dollars in grant funding in efforts to accomplish improved energy policy, public incentive, education and outreach programs, and energy security.

Colorado Legislation and Activities

The progressive legislative activities that occur drive the processes for attaining any political goal. Below are selected legislation and activities that were crucial to moving Colorado into the forefront of renewable energy expansion. For the full legislative framework see Section XII – References.

- 2004, Amendment 37: The outcome of Colorado voters approving the first ever Renewable Energy Standard (RES), which requires that qualifying Colorado utilities generate 10% of their electric supply from renewable energy sources by 2015. Colorado was the first state in the nation to require a renewable energy standard.

- March 2007 - HB 1281 Increased Renewable Energy Standards from 2004 Amendment 37. Establishes the Following Standards

Date	Investor Owned Utility	Rural Coops & Municipal Utilities
2008-2010	3 to 5%	1%
2011-2014	6 to 10%	3%
2015-2019	10 to 15%	6%
2020	10 to 20%	10%

- April 2007, Executive Order D011 07: *Greening of State Government* - requiring state agencies and departments to reduce overall energy use in all state facilities by 20% or more no later than the end of fiscal year 2011-2012.
- November 2007, the Colorado Climate Action Plan was published laying out a path to reduce greenhouse gas emissions 20 percent by 2020.
- 2007, SB 07-091, CRS 40-4-116: Creates the 16-member Renewable Resource Generation Development Area Task Force to develop a map of existing generation and transmission lines and areas in Colorado with potential to support competition among renewable energy developers for renewable energy projects.
- 2007, SB 07-100, 40-2-126: Establishes Transmission Incentives to Energy Resource Zones.
- July 2008 Governor’s Energy Office Sustainability Policy: Proposed goals to reduce energy consumption by 20%, water consumption by 10%, petroleum consumption by 25%, paper consumption by 20%, and to divert 75% of waste from landfills by June 30, 2012 (based on a baseline of SFY 2005-06).
- 2009, SB 09-297, CRS 40-2-124 – *Renewable Energy Standard (as amended)*: Concerning incentives for the installation of new distributed renewable energy generation facilities in Colorado increasing the target percentages under the electric utility portfolio standard to encourage Colorado utilities to generate three percent of their retail electricity sales from distributed renewable sources by the year 2020 adopting standards for the installation of distributed solar electric generation equipment, and making an appropriation therefore.
- April 2010, HB 1365, CRS 40-3.2-201- *Clean Air-Clean Jobs Act*: Incentivize Utilities to Convert Coal to Natural Gas. Concerning incentives for electric utilities to reduce air emissions, and, in connection therewith, requiring plans to achieve such reductions that give primary consideration to replacing or repowering coal generation with natural gas and also considering other low-emitting resources, and making an appropriation.

- November 2010, HB 1001, CRS 40-2-121: Increase of 10% for investor owned utilities to 30% by 2020.

Date	Investor Owned Utility	Rural Coops & Municipal Utilities
2007	3%	1%
2008-2010	5%	1%
2011-2014	12%	3%
2015-2019	20%	6%
2020 Forward	30%	10%

- November 2010, HB 10-1342, CRS 40-2-127: Encourages additional investment in Solar Energy creating Community Solar Gardens
- Adopted 2010, SB 11-131, CRS 40-4-118: *Creation of the Colorado Smart Grid Task Force* - The Task Force’s primary task is to produce a report containing recommendations and analysis on the feasibility, cost, and timing of transitioning to a secure, resilient, and technologically advanced electric grid, also referred to as the “Smart Grid”, in Colorado for the use by Colorado residents, business and governmental agencies.
- March 2010, SB 10-174, CRS 37-90.5-102: *Geothermal Resources Act* - The development of geothermal resources is in the public interest because it enhances local economies and provides an alternative to conventional fuel sources.
- 2010, HB 10-1328, CRS 32-20-101 - *New Energy Jobs Creation Act 2010: Concerning the “New Energy Jobs Creation Act of 2010”*, and, in connection there with, creating the Colorado New Energy Improvement District and authorizing the district to fund new energy improvements by issuing special assessment bonds payable from special assessments levied on eligible real property owned by persons who voluntarily join the district in order to have the district help them fund new energy improvements to the eligible real property.
- 2011, SB 11-045, CRS 40.4.119: *New Electric Transmission Facilities* – Necessary to promote the development of additional clean and renewable electric generation resources.
- 2012, HB 12-1315: Changes the name of the *Office* from Governor’s Energy Office to Colorado Energy Office; establishes two funds: Innovative Energy Fund, and Renewable and Clean Energy Fund.

Summary

The State of Colorado has established itself in a frontline position as proactive in developing result-oriented energy solutions. As Colorado moves forward with energy legislation and sound strategies for all energy sectors, energy assurance best practices will become integrated into the daily functions of government operations and citizens’ daily activities.

V. Plan Maintenance Process

Maintenance of the Plan is critical to the overall success of energy assurance planning and is normally addressed as one of the final elements of the planning process. In this Plan structure, however, Plan Maintenance is brought to the forefront establishing an agreed-upon process for continued collaboration between entities. This section describes the State's system for updating the plan, monitoring activities, and maintaining a useful, working document.

Method and Schedule for Monitoring, Evaluating, Updating, or Revising the Plan

The DOE recommends updating an EA Plan on a three year cycle; however, the core EAAG (CEO, PUC, and DEM) will review the Plan annually and may update the Plan if critical updates are identified. CEO will initiate the review and coordinate revisions with the core EAAG initially and include industry, federal, state, city and county stakeholders as appropriate. A record of revisions will be kept with the plan. Any revisions will be submitted to DOE as a normal course of completion.

Actions that would instigate an evaluation, update or revision sooner than annually:

- An actual energy emergency or any disaster with impacts to the energy sector
- Political change or reorganization
- Legislative action relative to Energy Assurance Planning

Process may include but not limited to:

- **CEO**
 - Monitor industry activities and coordinate a quarterly meeting, a tri-task between CEO, PUC, and DEM
 - Quarterly meetings, a tri-task between CEO, PUC, and DEM, are to further explore the possibility for implementing any of the identified initiatives and actions in the Action Plan Mitigation Strategy. Note any implementation progress or deletion.
 - As a tri-task effort, record meeting minutes and communicate the schedule and activities for Plan updating and maintenance to stakeholders in advance, facilitating additional meetings if necessary
 - Maintain intergovernmental and interagency stakeholder coordination and outreach to interested parties and the public who may provide pertinent information for Plan update
 - Communicate energy assurance success stories and prepare progress reports if applicable
 - Monitor and update GIS Database annually
 - In the case of an energy emergency, plan for debriefing of the incident for lessons learned
 - Note priorities, regulations, policies, or procedures that may need modified
 - Build in-house redundancy by cross-training in case of position vacancy or absence
 - Monitor DOE and NASEO guidelines for aligning update with requirements

- Monitor legislation activities for implications on energy assurance planning
- **DEM**
 - As a normal course of action, DEM monitors and updates the SEOP. Should any incident occur that might have implications for ESF #12 operations or for the EA Plan, whether due to an incident or political activities, maintain information sharing best practices with co-lead agencies
 - Participate and help coordinate in the Plan review for update
 - Note results of any exercises or drills that may have energy sector implications to improve the Plan
- **PUC**
 - Maintain best practices information sharing with CEO and DEM on related energy sector issues and successes for incorporation into the Plan update, if applicable
 - Participate and help coordinate in the Plan review for update
 - Note results of any utilities exercises or drills that may have energy sector implications to improve the Plan

Table 2 Record of Revision Table

Change #	Agency	Pages, Paragraphs, Sections Modified	Date

VI.Recommendations: Problem – Solution – Evaluation

Recommendations are also normally addressed as a closing element of a planning process. Many excellent ideas and innovative approaches were realized throughout the EA planning process and are showcased here as an opportunity for future consideration. Also due to the quality and efficiency of energy conservation programs analyzed from other states, a selection is outlined here as a recommendation for consideration in Colorado. They are organized by alignment with the four Overarching Goals of the Plan and stated as Problems and Potential Solutions.

Overarching Goals

- 1) Provide Public Welfare and Protect Critical Infrastructure
- 2) Improve Communication, Coordination, and Public Information
- 3) Expand and Improve Energy Assurance Awareness through Educational Outreach
- 4) Improve Investment for Appropriate Reliability, and Resiliency

Problem 1: Coordination and Collaboration <i>Aligns with Goal 2: Improve Communication, Coordination, and Public Information</i>
Potential Solution: New Conservation Program

Perks for Voluntary Conservation Efforts

More than the Energy Star program – develop a complimentary program to Energy Star that offers reward prizes either in rebate dollars or in the form of gift cards for essentials like groceries, gas, etc. for a reduction in energy kW usage from prior years bill to current years bill as long as it’s in the same location. There could be collaboration with utilities provider that advertises how the program works through their website or in their bill. Perhaps the utility provider would be interested in funding part of the perks in other conservation encouraging ways, such as, a “pilot smart meter program” or a “community solar garden program” for those that want to participate in the conservation perks program; then once consistent communityconservation efforts are recorded, their level of perks increase. Such as in a brown out or black out – their power stays on as long as their location can be islanded from the grid. It’s likened to air travel miles - the more you fly the more flying is free.

Potential Solution: WebEOC Access for Utilities (under consideration)
--

Outage Tracking Enhanced Capability

Through the EA Planning process, WebEOC, a disaster management software tool used by emergency management practitioners during real events or in exercises to track the specifics of the disaster, was suggested as a potential tool for utilities. It would allow the utilities to input outage information and expected restoration timeframe into the system during an actual event. The jurisdictions impacted, as long as they were a participating jurisdiction with WebEOC access, could be informed earlier and make more accurate response and recovery decisions related to power outage and vulnerable populations.

The suggestion has been made to the appropriate decision-maker and is currently being explored.

For comparison, the WebEOC tool for utilities could be as advantageous as the Hazard Map Overlays were in the recent, Lower North Fork wildfire in Jefferson County. Energy assets have been plotted on maps that show selected natural hazard zones by county. Officials could look at the wildfire hazard map for Jefferson County, determine energy assets proximity to the wildfire, and make appropriate decisions about critical infrastructure protection, evacuation, and other necessary response activities.

Other Potential Programs/Solutions for Problem # 1

- Attend and/or hold Exercises and Conferences (i.e. Critical Infrastructure Protection Conference; Regional Energy Emergency Exercise)
 - Prioritize key threat/disaster scenarios relating to CI and develop exercise scenarios
 - Develop exercise target schedule
- Identify infrastructure outside the state that is critical to the State, and if necessary, ways to assure and/or enhance its protection
 - May be as simple as for owners/operators of infrastructure to communicate their recognition of Washington’s concerns, and report on its protection.

Problem 2: Educational Outreach for Energy Assurance Awareness
Aligns with Goal #3
Expand and Improve Energy Assurance Awareness through Educational Outreach

Potential Solution:
Energy Conservation Public Outreach TV Commercial

Unplug Before Bed

The best source for conservation is the average residential consumer. Although it appears to be inconvenient to unplug unnecessary electronics and appliances as a regular course of “end of the

day” activities, consumers who view a commercial enough times where a family unplugs before bed, a new habit can become a part of the daily routine without much encouragement. There are conservation commercials nationwide, but one of the most effective is a commercial shown on the East Coast by Touchstone Energy Cooperatives where the family is brushing their teeth before bed and the last thing they do (as a part of their end of the day regimen) is go through the house unplugging unnecessary electronic items. This commercial is very well-done and tasteful. It is recommended that the State of Colorado contact Touchstone Energy Cooperatives at 703-907-5742. The Director of Communications and Membership is Ann Maggard; Senior PR and Education Advisor is Amy Rosier.

Potential Solution:
Energy Sector Fact Sheets (under development)

Energy Sector Fact Sheets for CEO website

Informational Fact Sheets about each energy sector are currently being designed to post on CEO’s website as an educational tool for Colorado citizens.

Other Potential Programs/Solutions for Problem # 2

- Develop educational programs with incentives for demand reduction strategies
 - Demand Reduction Strategies
 - Reduce travel
 - Hold fewer public events
 - Provide increased transit services to public events
 - Turn down thermostats
 - Substitute products (i.e. hydrogen)
 - 65 degree heating in State buildings and 105 degree hot water temps
 - Add Energy Assurance Awareness element into existing public outreach programs
- State assistance for Local Energy Assurance Plans

Problem 3: Reliability (Conservation) and Resiliency (Continuity) specifically Critical Infrastructure and Cyber Security
Aligns with Goal # 1
Provide Public Welfare and Protect Critical Infrastructure
Aligns with Goal #4
Pursue Appropriate Reliability and Resiliency

Potential Solution:
Monitor and Update GIS Database and Hazard Overlay Maps

Monitor and Update GIS Database and Hazard Overlay Maps

The GIS database is a comprehensive log of energy sector assets in Colorado. They are plotted on an interactive web based Geographic Information Mapping System that allows officials to utilize the information for planning and other purposes.

Recommendation: CEO designate a responsible party to monitor and update GIS Database ascertaining that new assets are also plotted on the hazard overlay maps.

Potential Solution:
Extensive multi-year, multi-disciplinary, mixed methodological study on “willingness” to do what it takes to conserve electric energy

Extensive multi-year, multi-disciplinary, mixed methodological study on “willingness” to do what it takes to conserve electric energy

- **Research and Development**

- Partnership with an educational entity for data collection. Utilize existing partnerships if possible.
- Developing questions
 - What are the questions that CEO wants to know?
- Sampling Technique
 - Need to decide who the population is. Is it all residents of Colorado? Is it homeowners? If you’re going to do a study of this size, would you consider business owners as well? How would you distinguish the two when you get the data back? What is the population? Whatever it is, how are you going to get them to participate in the study? Is there an incentive to participate?
- Focus groups:
 - Two or three small groups of the sample are chosen to ask the relevant questions to; who will then discuss in a group the answers to the question(s). Focus groups are good when there aren’t enough questions to justify an individual interview with each participant, but they are still qualitative questions. They are also good because groups can pull information out of other group members, and collaboratively come up with solutions that were not considered otherwise.
- Quantitative Survey
 - Create a survey questionnaire based on the information received from the focus groups, and obtain a sample large enough to gain statistical power (taking potential non-response into consideration) to verify whether the information found in the focus groups is representative of the rest of the population of interest.
- Compilation and analysis
 - Enter, clean, and analyze the data

- **Planning**

- Decide what the best solutions are, based upon the results of the research analysis
- Develop programs around those solutions

- Assess the investment and potential return on the investment (ROI)
 - The potential return may include potential reduction in energy consumption per household
- Research funding sources
- Secure funding
- **Implementation**
 - Implement programs
 - Encourage state and local participation in like programs
- **Evaluation**
 - Program Evaluation

**Potential Solution:
Implement Programs Successful in Other States**

- Energy Outage Data Collection and Analysis
- Automated outage reporting system
- Monitor energy disruptions
- Tracking systems
- Incentives for Alternative Transportation (i.e. public transportation or bicycle)
- Solar water heating systems
- Replacement heating equipment program Clean Energy incentives
- Temperature restriction programs (state buildings)
- Research and development for GIS maps
- Alter Parking availability
- Incentives to encourage proper vehicle maintenance/vehicle efficiency
- Programmable thermostats: encourage higher summer temps and lower winter temps
- Incentives to private stations (E85 and B20 tank installation, research and develop E15-E40)
- Plug-in hybrid electric conversion rebate program
- Alternative fuel vehicle program
- Implementation of Smart Grid
- Reduced lighting (state buildings)
- Increase petroleum prices to reduce usage (Idaho)
- Add HOV lanes
- Encourage federal funding of research and development of all technologies that can provide base-load power while achieving reduced CO2 emissions
- Cash incentives to reduce upfront costs for business programs (i.e., installing programmable thermostats, or participating in a compressed work week, or implementing temp “restrictions,” etc.)
- Kill-A-Watt Electricity Monitors – help find which appliances (etc.) are stealing the most power

- Research and Development on Cyber Security programs
- Visitor Screening Guidelines for Cyber Security (utilities and others)
- Buffer Zone protection program: DHS risk assessment program that attempts to identify vulnerabilities to areas surrounding CI. DHS contractors work with energy companies and local law enforcement to implement the program and report findings and recommendations to the companies.
- Encourage The Half Project (this shows a resident how to cut their energy bill in half, but the resident must be willing to have some inconveniences)
- Truck Driver hour waivers /Varying work hours
- Telecommuting
- Speed limit reduction and/or strict enforcement
- Fleet management routing and scheduling (public and private)
- Phasing traffic lights to conserve fuel energy
- Energy code compliance and monitoring

<p>Problem 4: Redundancy (Preparedness, Recovery, and Resource Sharing) <i>Aligns with Goal #4</i> <i>Pursue Appropriate Reliability and Resiliency</i> <i>(Building redundancy measures provide operational reliability)</i></p>
<p>Potential Solution: Encourage Utilities to Support the Spare Transformer Equipment Program (STEP) with Edison Electric Institute</p>

Encourage Participation in the Spare Transformer Equipment Program (STEP) with Edison Electric Institute:

This program is a sharing agreement, which is a binding contract between all participants that conveys the governance of the program. It was developed with the input from more than 50 utilities. Participating utilities commit to share spare transformers if a “triggering event” occurs. FERC has issued orders approving participation and cost recovery. This program is open to any transmission owner.

March 2012, DHS in collaboration with the utilities industry and the Electric Power Research Institute constructed a “Drill to Replace Crucial Transformers.” The drill cost approximately \$17 million.

Recommend: Collaborate with Utilities and DHS to design drills and exercises that practice supply chain and transformer replacement functions.

Problem 5: Energy Emergency Recovery
Aligns with Goal #1
Provide Public Welfare and Protect Critical Infrastructure

Potential Solution:
Implement Programs during Liquid Fuels Energy Shortage
(Potential recovery programs listed below are for mandatory conservation in the case of a serious liquid fuels shortage event)

- Fuel Set-Aside (State and industry)
- Increased storage capacity for petroleum products
- Increased storage for natural gas (e.g. LNG)
- Back-up generators and long period fuel storage
- Develop a weight restriction waiver strategy for delivery or distribution of energy related products over the State’s highway system
- Fuel Allocation - odd/even day gasoline purchase
- Compressed work/school weeks
- Suspended blend wall for petroleum (% ethanol in fuel) in times of emergency
- State-wide escalation of emergency measures to reduce energy consumption during an electric outage or disruption
 - Such as closing schools, offices, factories
 - Lower minimum building temperatures
 - Relax delivery requirements such as highway usage or pipeline
 - Guarantee utility access to key assets (e.g. poles on government property)
 - Relax emission requirements

Recommendation: Identify and Plan for potential emergency recovery programs to be implemented for mandatory conservation in the case of a serious energy sector shortage, outage, or disruption event.

Any program implemented should also have an evaluation process to determine its level of success for continuation or elimination.

VII. Conclusions

Throughout the near two-year EA Planning process, many lasting relationships have been built between State, Local, and Federal agencies, the private sector utilities and associated businesses, municipal utilities, and many other stakeholders. Bringing emergency management practices to the table with utilities operations has enriched Colorado's understanding of the complex issues surrounding energy related emergencies. The EA Initiative has allowed an opportunity for State agencies to look at the energy sector with a new set of eyes where appreciation for collaboration and information sharing that occurred cannot be overstated. The State of Colorado is more prepared because of it.

In conclusion, the most significant accomplishments from this process:

- Building relationships between energy sector stakeholders and State government by organizing the EAAG
- Developing the EA Hierarchy establishing a framework for communication between the energy sectors and State agencies involved in disaster management
- Clearer understanding of the threats, risks, vulnerabilities and interdependencies across the energy sector and how they relate to emergency management preparedness, response and recovery – specifically cyber networks vulnerabilities and their interconnectedness
- Conducting the first Geomagnetic Exercise in partnership with NOAA's SWPC and the information gathered as a result of the exercise helped to sculpt a platform for responding to HILP events
- Identifying the capability gaps relative to energy emergencies management
- The understanding and appreciation of the utilities operational processes during an energy emergency and during the normal course of business; and likewise the clarification of government processes related to emergency and disaster management, which identified the roles and responsibilities of each
- Selecting overarching goals for the plan
- Recognizing potential solutions to close the capability gaps
- Developing an energy sector GIS Database and Natural Hazard Overlay Maps as a tool for critical infrastructure protection
- Integrating a schedule for quarterly Energy Assurance Planning meetings

The State of Colorado would like to extend a sincere thanks to all participants and stakeholders for their support and willingness to stay engaged throughout the EA Planning process and look forward to utilizing the tools that have been developed toward improving Energy Assurance both statewide and regionally.

Book 2

Energy Assurance Action Plan

The Energy Assurance Action Plan is a compilation of four separate strategies: Response, Recovery/Restoration, Mitigation and Public Information. Together they establish a platform for streamlined communications and operations during each phase of an energy emergency event.

Book 2 Table of Contents

VIII. Energy Assurance Emergency Action Plan	1
Introduction	1
Response Strategy	2
Recovery/Restoration Strategy	24
Mitigation Strategy	44
Public Information Strategy	69

The CEAEP is a comprehensive document that includes background information, reference materials, and other subject matter that may not be of interest to all readers. As a convenience, suggested sections are identified below for specific audiences.

For State Agencies and Local Emergency Management Stakeholders

- All Strategies

For Utilities

- All Strategies

This Page Left Intentionally Blank

VIII. Energy Assurance Emergency Action Plan

Introduction

The Energy Sector, as identified in the National Infrastructure Protection Plan (NIPP) and defined in Homeland Security Presidential Directive -7 (HSPD-7), consists of thousands of electricity, oil, and natural gas assets that are geographically dispersed and connected by systems and networks. Due to its systems interdependency, an impact to one sub-sector can potentially affect all other sub-sectors. A shortage, disruption, or outage of power or fuel delivery and the management of such constitutes an energy emergency (EE) at any level. An EE can be a stand-alone incident or one element of a larger disaster event. The Energy Assurance Action Plan (EA Action Plan) is a series of strategies developed by the Energy Assurance Advisory Group (EAAG) to serve as an operational platform that accentuates collaboration between the energy sector and State and local government agencies and focuses on energy sector issues. It consists of three separate, major strategies; one to cover each phase or operational period of an emergency; 1) Response, 2) Recovery and Restoration, and 3) Mitigation. The fourth strategy, Public Information, is complimentary to the first three. Having a Public Information strategy is essential throughout the duration of an incident emphasizing the accuracy of the information disseminated and the appropriate distribution channels.

Each strategy is self-directing and can be used separately or they can function as a comprehensive EA emergency action strategy developed in efforts to achieve the overarching goals of the Plan. Whether the initial damaging impact is caused by natural disaster or human-caused, the complexities associated with the energy sector are unique and require a broader understanding of the processes involved among energy stakeholders and which may change from one phase or operational period to another. Once primary capability gaps were identified, such as *improve communications*, and associated to the proper emergency phase or operational period, each strategy could be tailored to address a primary gap accordingly. The third major strategy, Mitigation, does not normally accompany an *emergency* plan as it is considered a planning mechanism used to reduce future impact; however, because the EA planning process is designed to identify areas for improvement and discuss potential solutions, it was found that many of the potential solutions would require a comprehensive feasibility and return on investment (ROI) analysis for any consideration for implementation. Therefore, all capability gaps are listed in the Capabilities Gap Analysis, as well as the potential initiatives that could provide solutions to address the gaps. The potential initiatives are categorized respectively under the four overarching goals of the Plan and presented in a table at the end of the Mitigation Strategy. The overall Plan is a living document to be used, modified, updated, revised, and maintained. The Mitigation Strategy is included as a value-added component. The potential initiatives can be further explored in the quest for improving energy reliability, resiliency and redundancy.

Response Strategy

The EA Response Strategy is based on agreed-upon response actions among the members of the EAAG as a result of the EA planning process.

There are various energy scenarios that will necessitate a response from Emergency Management and their energy sector partners. Some main scenarios are:

- **Energy Shortage Management:** This mitigates the occurrence of crises resulting from the shortage of any vital resource as a consequence of interruption or shortage of electricity, petroleum products, natural gas, propane gas, or any of the resources used in the generation of electricity.
- Incoming threats to critical infrastructure including atmospheric and space weather phenomena may necessitate pre-incident preparedness actions to lessen any anticipated impact.
- Interruption or cessation of electrical output through systems failure or an intentional or deliberate act to disrupt would necessitate immediate response actions to manage cascade system failures and secondary impacts.

When it is not possible to avert a crisis, it is imperative to take such actions as are necessary to ensure the health, safety, and welfare of the citizens of the state. Vital resources are defined to include food and water for domestic use, water for agricultural or industrial use, and water for electric power generation, petroleum based fuels, uranium, coal, natural gas, propane gas, or any other form of energy.

The actions identified in the response strategy are primarily electric sector specific with relative natural gas infrastructure impacts. The updated Liquid Fuels Plan is referenced in a later section and is provided in full in the appendices.

Purpose

The purpose of this strategy is for the activation of a systematic framework that provides timely and coordinated response actions during an electric energy disruption or outage to streamline and mobilize resources so that pre-event conditions of society can be efficiently restored.

Overarching Plan Goals

- Provide Public Welfare and Protect Critical Infrastructure
- Improve Communication, Coordination, and Public Information
- Expand and Improve Energy Assurance Awareness through Educational Outreach
- Improve Investment for Appropriate Reliability, and Resiliency

Authority

- State
 - Title 24, Article 32, Part 2101 et. Seq., Colorado Revised Statutes, as amended; entitled the *Colorado Disaster Emergency Act of 1992*.
 - Article IV, Constitution of the State of Colorado; entitled the *Executive Department*.
- Federal
 - Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. §§ 5121-5207).
 - The National Response Framework, January 2008.
- Utilities
 - North American Electric Reliability Corporation (NERC)
 - Standards Process Manual (available online at http://www.nerc.com/fileUploads/File/Appendix_3A_Standard_Processes_Manual_Rev%201_20110825.pdf)
 - Reliability Standards <http://www.nerc.com/page.php?cid=2|20>
 - Communications (COM-001 through COM-002)
 - Critical Infrastructure Protection (CIP-001 through CIP-009)
 - Emergency Preparedness and Operations (EOP-001 through EOP-009)
 - EOP-002-2 Capacity and Energy Emergencies – ensures Reliability Coordinators and Balancing Authorities are prepared for capacity and energy emergencies
 - Event Analysis Program (revised February 21, 2012) – analysis of operations, planning and critical infrastructure protection processes

Scope

The EA Plan uses an all-hazard, whole community approach addressing a full range of complex requirements surrounding energy emergencies. It details the specific incident management roles and responsibilities of State departments and agencies as well as the private utilities stakeholders that may be involved in response and recovery operations of an energy emergency. It establishes a system for collaborative communication between State and local government and private utility stakeholders with the intent to streamline accurate information to the Governor and assist in expediting the recovery of societal functions to a state of normalcy.

EA Response Best Practices

- To provide a systematic response framework for expedited collaboration between private/public electric and natural gas utilities, State and local government agencies, and other response support agencies during an energy disruption or outage event
- To consider the interdependent network systems between energy specific sectors in anticipation of cascading failures due to an energy disruption or outage
- To establish roles and responsibilities unique to the complexities of an energy emergency
- To expedite the delivery of accurate disruption or outage information to the Governor
- To disseminate public safety information by activating the Joint Information System (JIS)

- Coordinate requests for assistance through the ESF framework of the SEOP
- Mobilize response resources
- Leveraging technologies to increase pace and efficiency of response
- Systematically prioritizing response processes to avoid redundant efforts and reduce recovery costs

Planning Situations and Assumptions

Situations

- Widespread and prolonged electric power outage may occur
- Transportation and telecommunications infrastructures may be affected
- Interdependent network systems affected may cause a series of cascade failures
- Delays in the production, refining, delivery of petroleum-based products may occur as a result of loss of commercial electric power
- Damage to an energy system in one geographic region may affect energy supplies in other regions that rely on the same delivery systems. Consequently, energy supply and transportation concerns can affect Intra-State, Inter-State, and/or International regions.
- Loss of continuity of power becomes an increased threat to critical services and may create significant degrees of human suffering, property damage and economic hardship to individuals, governments, the environment, and for the business community.
- Local government operations may be compromised or severely impacted
- Secondary impacts (i.e., fires, hazardous materials, explosions) could imperil responders, hinder response operations, and become a public safety consideration
- Outage or disruption may potentially be the result of an act of terrorism which necessitates precaution to preserve evidence
- Economic impacts will be felt immediately throughout the impacted region. These impacts will increase exponentially as the outage continues.

Assumptions

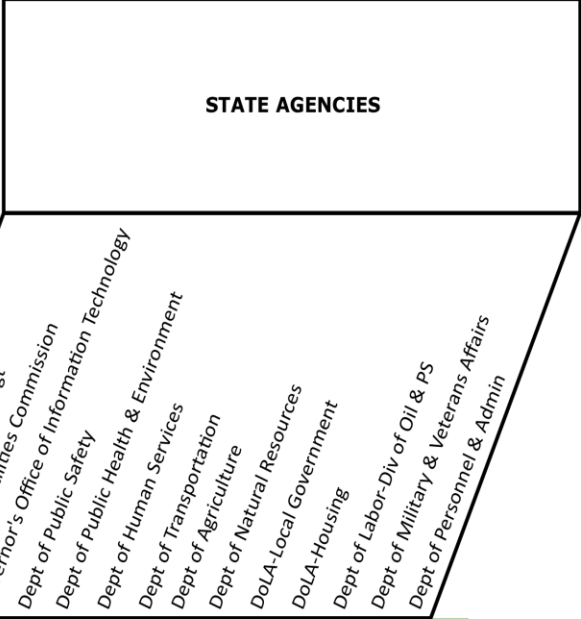
- Local, State and Federal government share in the responsibility to respond to and recover from an energy emergency
- Government must continue to function in delivering critical services
- Information sharing must occur between public and private entities and across all levels of government
- Redundant power generation capability and fuel reserves may be required for continuity of critical State and local services such as:
 - Public Works
 - Water/Waste Water systems
 - Mass Care and Public Health
 - Critical Care facilities

- Public Safety
- Law Enforcement, Fire and Emergency Medical operations
- Communications
- Transportation systems (mass transit, traffic lights, etc.) which rely on electric power will be impacted causing massive traffic congestion and may need search and rescue operations and/or alternative transportation means
- Agriculture and Food sector will be severely impacted (i.e., food spoilage, meat and dairy operations, grain processing)
- Banking and Finance sector communications capabilities will be compromised
- Natural Resources sector may be affected
- Dams
- Renewable Energy Operations
- Fossil Fuels extraction processes

Response Function Matrix

Figure VIII-1 below is a matrix that identifies the general functions conducted during the response phase or the first operational period of an energy emergency and the agencies that perform those functions. This is to highlight that both public and private energy sector stakeholders conduct similar activities within their own operational processes, but can collaborate through liaison improving overall response. On the other hand, some functions are specific to a certain organization, such as feeding and sheltering, which are responsibilities associated with the American Red Cross and other organizations like the Salvation Army.

This Page Intentionally Left Blank



MAIN FUNCTIONS	Colorado Energy Office	DoLA-Div of Emergency Mgmt	DoRA-Public Utilities Commission	Governor's Office of Information Technology	Dept of Public Safety	Dept of Public Health & Environment	Dept of Human Services	Dept of Transportation	Dept of Agriculture	Dept of Natural Resources	DoLA-Local Government	DoLA-Housing	Dept of Labor-Div of Oil & PS	Dept of Military & Veterans Affairs	Dept of Personnel & Admin
assess incident	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
secure critical infrastructure					x			x	x	x					x
→ security or perimeter protection					x										x
initial critical infrastructure damage assessment	x	x	x	x	x	x	x	x	x		x		x	x	x
→ assess essential transportation systems															
• traffic control					x										
→ assess energy assets impacts	x		x												
• assess outage or disruption			x												
→ communications systems analysis				x											
→ assess water resources systems						x				x	x				
→ assess waste water resource systems						x									
→ state services & state facilities assessment					x	x	x								
• assess state medical facilities impact/back-up power					x										
• assess government services															
→ assess agriculture and food sector									x						
public health & environment impact assessment						x									
→ medical triage						x									
→ access and functional needs populations assessment						x									
→ fatalities management						x									
→ food contamination						x									
→ air quality						x									
notification and reporting	x	x	x	x	x	x	x	x	x	x					x
→ briefing to the Governor	x	x	x	x	x	x	x	x	x	x					x
implement or activate an emergency plan	x														
→ public information plan activation	x	x	x		x	x	x	x	x	x					x
activate emergency operations center		x			x		x	x							x
stakeholder coordination	x	x	x	x	x		x	x	x	x	x	x			
→ provide liaison	x	x	x	x	x	x	x	x	x	x	x	x			x
immediate incident response planning	x	x	x	x	x	x	x	x	x	x					x
→ mission tasking/event tracking	x	x	x	x	x	x	x	x	x	x					x
→ resource mobilization and management		x		x	x	x	x	x	x	x					x
• debris management		x			x		x								
finance documentation	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
mass care, housing and human services							x					x			
→ sheltering							x								
→ feeding							x								
→ bulk distribution							x							x	
victim services					x	x	x		x				x	x	

ENERGY SECTOR STAKEHOLDERS														LOCAL AGENCIES							
Electric Utilities					Natural Gas			Liquid		NGOs											
Regulated		Unregulated																			
Xcel Energy																					
Black Hills																					
TriState																					
Colorado Rural Electric Assn																					
Xcel Energy																					
Black Hills																					
Colorado Natural Gas																					
Colorado Oil and Gas Assn																					
American Red Cross																					
Salvation Army																					
Colo Voluntary Org																					
Active in Disaster																					
local emergency management																					
local law enforcement																					
local fire department																					
local emergency medical or public health																					
local utilities																					
local road & bridge																					
local public works																					
local environment																					
local information technology																					

X	X	X	X	X	X	X	X	X	X	X										X	X	
X	X	X	X	X	X	X	X	X												X	X	X
X	X	X	X	X	X	X	X	X														
X	X	X	X	X	X	X	X	X														
X	X	X	X	X	X	X	X	X														
X	X	X	X	X	X	X	X	X														
X	X	X	X	X	X	X	X	X														
X	X	X	X	X	X	X	X	X														
X	X	X	X	X	X	X	X	X														
X	X	X	X	X	X	X	X	X														
X	X	X	X	X	X	X	X	X														
X	X	X	X	X	X	X	X	X														
X	X	X	X	X	X	X	X	X														
X	X	X	X	X	X	X	X	X														

Roles and Responsibilities

Introduction

Clarification of primary Energy Sector stakeholders’ roles and responsibilities are bulleted in the table below. Clarifying the operational processes among stakeholders improves communications and provides opportunity for continued collaboration.

Office of the Governor
<ul style="list-style-type: none"> ✓ Authorized to activate the SEOP under 24-32-2104(5) CRS through the issuance of an Executive Order. <ul style="list-style-type: none"> ○ May include the activation of the National Guard

Colorado Division of Emergency Management
<p>The State Emergency Operations Center (SEOC) can be activated at any time by the DEM Director or their designated representative.</p> <ul style="list-style-type: none"> ✓ The function of the SEOC is to provide assistance to local jurisdictions. This assistance takes the form of: <ul style="list-style-type: none"> ○ Providing Statewide situational awareness ○ Coordinating State, local, Federal and private sector resources that the impacted jurisdiction(s) need to respond and recover from a natural, technological, or human-caused incident. ○ Documenting and routing resource requests • Declaration process <ul style="list-style-type: none"> ○ Disaster/Incident occurs ○ Local declaration and request for State assistance ○ DEM receives local declarations and makes recommendation to Governor’s Office for a state disaster emergency ○ A disaster declaration allows the Governor to reallocate funds to the Disaster Emergency Fund ○ Governor requests federal assistance • Assist in coordination and information sharing. <ul style="list-style-type: none"> ○ Primary role is to support in-house utility response by providing utilities with information and coordination support. ○ Not necessary to have Utility representative at the SEOC, though recommended. WebEOC can be used virtually to input information relative to a disaster event and track its requests, resources, and other critical information. • The SEOP is an ESF structure that is in place to handle energy-related issues. DEM requests State Agency ESF representatives (of the affected sectors) to respond to the SEOC to assist in coordinating the response.

Colorado Energy Office & Public Utilities Commission
(Co-Lead Agencies for ESF#12)

During An Event

- ✓ ESF #12 - Energy has a co-lead structure. The Colorado Energy Office (CEO) and the Public Utilities Commission (PUC) will be requested to respond to the SEOC.
- ✓ CEO and/or the PUC activates the Colorado Energy Assurance and Emergency Plan (CEAEP)
 - Activate CEO/PUC Public Information Plan and establish early coordination with the Joint Information System
- ✓ Maintain contact with all energy-related organizations, companies, and special districts.
- ✓ Share responsibilities for the collection and evaluation of information on energy system damage. The term “energy” includes producing, refining, transporting, generating, transmitting, conserving, building, distributing, and maintaining energy systems and system components.
- ✓ May be asked to provide initial estimations on the energy sector impact, an anticipated restoration timeframe, areas affected by the disruption, and the percentage or number of residential and business entities without services.
- ✓ Maintain communication with all energy-related organizations, companies, and special districts during restoration operations to communicate to the SEOC any need for recovery assistance by the State such as debris removal for repair crews. This would be coordinated with other ESF’s participating within SEOC.
- ✓ Additional personnel may be requested by CEO and the PUC to respond to the field or to the SEOC to assist with gathering current information for support to emergency operations.
- ✓ Assistance in tracking information from the utilities’ coordination of interstate resources (i.e. equipment from utilities of other regions/states via Mutual Aid Agreements, etc. that might be utilized for recovery operations.
- ✓ Coordinate with the utilities involved to implement recovery strategies identified in the CEAEP.
- ✓ Provide periodic utility recovery status information during SEOC briefings so that current information on power restoration can be made available to local emergency offices via the WebEOC tool or through the JIS.

Colorado Energy Office & Public Utilities Commission
(Co-Lead Agencies for ESF#12)
During Normal Operations

- ✓ As co-lead agencies in ESF #12, the CEO and the PUC are required to fulfill the following duties:
 - If applicable, the Emergency Response Coordinator (ERC) is the lead agency representative for a specific ESF as outlined in the SEOP.
 - ERC will provide support through staff, technical services, and/or equipment to other ESF lead agencies.
 - Occupy a seat at the SEOC during the Center's activation.
 - Participate in SEOC exercises and associated training sessions, which may include WebEOC, SEOC management and forms usage, National Incident Management System (NIMS) training such as, All Hazard Incident Command System Command and General Staff Position-Specific Training.
 - During periods of non-activation of the SEOC, be aware of on-going incidents and relay applicable information to DEM (i.e., damage of electric transmission lines, power generating plants, transformers, natural gas pipeline, etc; or the correction of false reports in reference to infrastructure damage)
 - Assist in the periodic review and update of the SEOP due to lessons learned and/or new Federal guidance. Updates to the SEOP are conducted after:
 - An actual event in Colorado
 - An event elsewhere that would improve response
 - After exercises where the After Action Report (AAR) indicates corrective action is warranted to improve disaster operations.
 - Assist in pre-planning efforts for anticipated cascading natural hazards (secondary hazard impacts caused by the degradation from the primary hazard event)
 - Be a decision-maker for their respective organization
 - Have knowledge of, and work within the NIMS/Incident Command System, to include the Joint Information System.
 - The ERC should have a well established relationship with public and private utilities providers with 24/7 contact information points for secure information exchange, which establishes accurate situational awareness.
- ✓ Collaborate with the utilities to participate as "observers" in their disaster scenario exercises where opportunities to provide recommendations and share expectations for integrated communications can occur.
- ✓ Provide cross-training of in-house personnel

Utilities and Western Electricity Coordinating Council (WECC)	
Xcel Energy	<ul style="list-style-type: none"> ✓ Prioritize the critical users ✓ Restore power to the largest numbers and who has been out longest ✓ Identify areas of outage and work to prioritize response/recovery ✓ Contact local Emergency Managers ✓ Handle public information ✓ Report outage of a certain size to the PUC within 1 hour ✓ File their plan with NERC ✓ Provide a secure/redundant in-house EOC ✓ Provide for a secondary EOC at an alternate location
Black Hills Corporation	<ul style="list-style-type: none"> ✓ Track and report outages to WECC within 24 hours ✓ Monitors SCADA, Smart Meters and uses the Outage Management System ✓ Protects the main grid and equipment ✓ Restore power to their own infrastructure ✓ Provide a secure/redundant in-house EOC ✓ Provide for a secondary EOC at an alternate location
Tri-State Generation and Transmission Association	<ul style="list-style-type: none"> ✓ Follow FERC, NERC standards for reporting ✓ Reporting requirements are based on specific situational occurrences ✓ Report outages to WECC, if situation warranted ✓ Contacts local EMs when Tri-State facilities may be or are impacted. <ul style="list-style-type: none"> ▪ Have facilities in four states, one in Westminster, CO ✓ Have own coal production capability
Western Electricity Coordinating Council (WECC)	<ul style="list-style-type: none"> ✓ Maintain a reliable electric power system in the Western Interconnection. (The Western Interconnection stretches from Western Canada south to Baja California in Mexico, reaching eastward over the Rockies to the Great Plains.) ✓ Assure open and non-discriminatory transmission access among Members ✓ Provide a forum for resolving transmission access disputes between Members ✓ Act as a coordinating entity for the entire West Interconnection for activities of regional organizations with responsibilities for reliability and market functions ✓ Develop and adopt reliability, operating and planning standards, criteria and guidelines necessary to maintain the reliable operation of the Western Interconnection's interconnected bulk power system ✓ Certify Grid Operating Entities in the Western Interconnection ✓ Ensure that interconnected bulk electric system reliability assessments are conducted as needed ✓ Implement the Reliability Management System ✓ Implement any enforcement mechanisms ✓ Develop coordinated planning policies and procedures for the Western Interconnection ✓ Review and assess Local Regional Entity planning processes

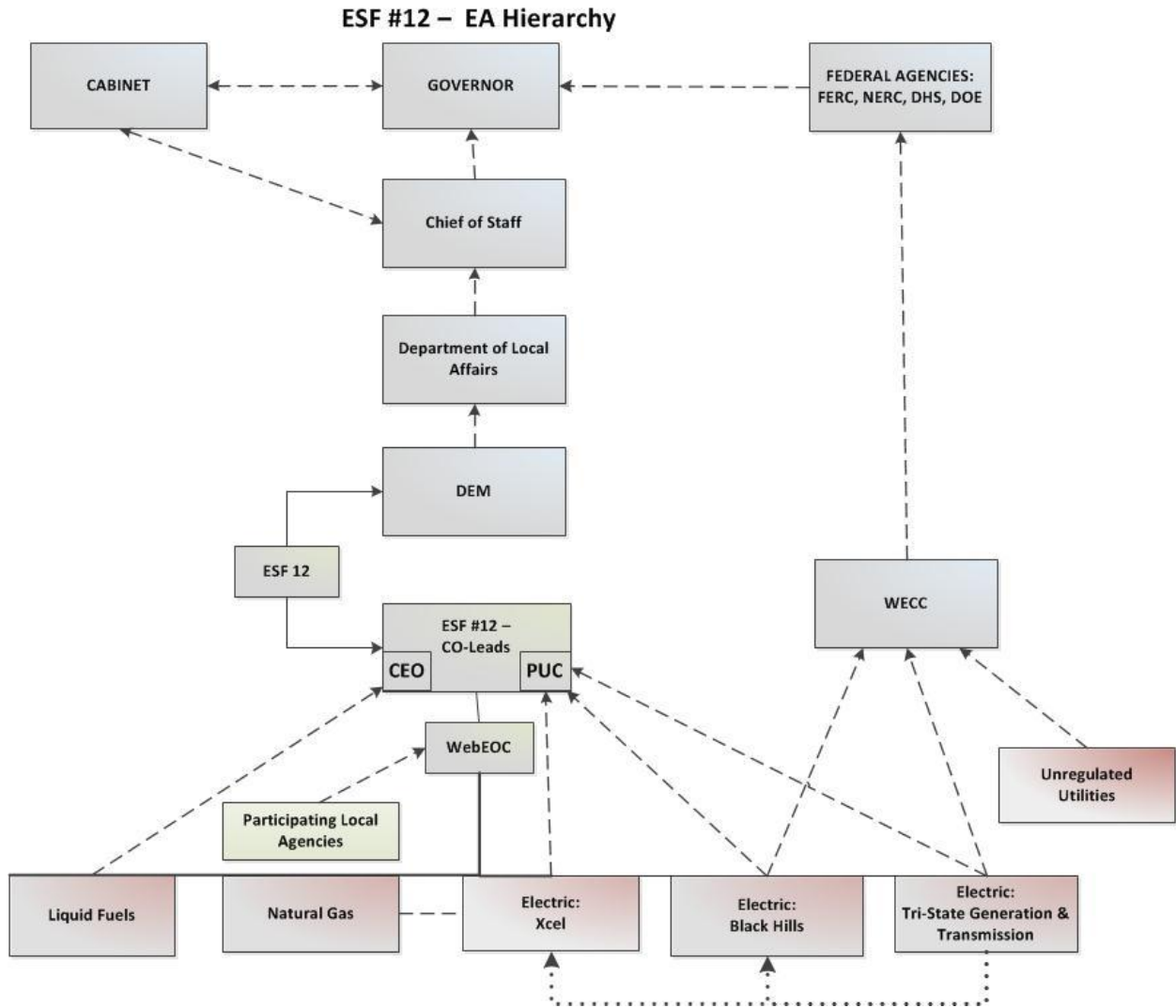
	<ul style="list-style-type: none"> ✓ Notify NERC, FERC, DHS, DOE, and WAPA ✓ Develop, coordinate and promote consistent interregional operating policies and procedures for the Western Interconnection, consistent with WECC/ERO standards and FERC policy ✓ Utilizes WECCnet for internal communications <ul style="list-style-type: none"> ▪ Regulated and non-regulated utilities communicate through WECCnet ✓ Resource dispatch capabilities between members ✓ Conduct annual exercises ✓ Act as the clearing house for outage information
--	--

Colorado Rural Electric Association	
Colorado Rural Electric Association	<p>Colorado’s Rural Electric Cooperatives (REC) purchase power and distribute it to their customers. Generation of power is critical as an external dependency, but not for direct protection by the Cooperatives. The REC’s focus on critical infrastructure lies largely with the transmission and distribution of power to consumers.</p> <ul style="list-style-type: none"> ✓ Assess impact ✓ Conduct Damage Assessment ✓ Repair and/or restore critical infrastructure ✓ Work with Division of Emergency Management on Damage Assessment Cost Analysis

Energy Assurance Emergency Hierarchy

The EA Emergency Hierarchy, Figure VIII-2, was developed by the EAAG to represent the operational process for ESF #12 during a state level disaster which impacts the energy sector. It is an organizational framework that establishes a course for communication, collaboration and liaison between public and private energy stakeholders during an energy emergency.

Figure VIII-2 ESF #12- EA Hierarchy



Continuity of Government

Each level of government should have the capability to preserve, maintain, and reconstitute its ability to carry out essential functions under the threat or actual occurrence of any disaster. Effective and responsive emergency operations are inseparable from the concept of Continuity of Government (COG). The Colorado program identifies two important factors for assuring continuity of government at the local and State level:

- Well defined and understood lines of succession for key officials and authorities
- Preservation of records and critical facilities which are essential to the effective functioning of government and for the protection of rights and interests of the State and its residents.

State Line of Succession

Article IV of the State Constitution of Colorado, establishes the emergency powers of the Governor and provides for the line of succession in the event the Governor is absent and/or unable to exercise the powers of office.

The legal successor to the Governor is the Lieutenant Governor. The following members (in order of priority) of General Assembly affiliated with the same political party as the Governor follow the state line of succession should the position of Lt. Governor be vacant and/or unable to exercise the powers of office.

- 1) Leader/Speaker of the Senate
- 2) Leader/Speaker of the House of Representatives
http://ballotpedia.org/wiki/index.php/Article_IV,_Colorado_Constitution

Other requirements

- Political subdivisions of the State shall be in accordance with the Constitution.
- State department heads shall designate primary and alternate emergency successors for key supervisory positions.
- Designated interim emergency successors shall be instructed on their responsibilities and the conditions under which they will assume these positions. They shall hold these positions until relieved by the Incumbent or until the emergency or disaster is manageable.

Provision of Essential Services

Provision for services that are determined as life sustaining and critical to the immediate economy of the State should have a system in place to maintain or restore such services immediately after a disaster event. Alternative or back-up facility(ies) should be designated that will allow for essential services to be provided. Each level of government is responsible for sustaining continuity of government operations.

Preservation of Essential Records

Protection of essential State and local records is vital to resume a functioning system of society after a major catastrophe or emergency. There are three categories of essential records and documents that need safeguarding

- Records that protect the rights and interests of individuals, which include vital statistics, State land and property records, financial and tax records, election records, license registers, articles of incorporation, and medical records
- Records required for effective emergency operations: plans, procedures, and resource inventories; lists of succession - regular and auxiliary personnel; , maps, agreements, contracts, and memorandums of understanding
- Records required to re-establish normal governmental functions and/or to protect the rights and interests of government, which may include federal and State laws, rules and regulations, official proceedings, financial and court records

Vital records should be duplicated and maintained in the safest accessible, yet remote location.

Concept of Operations

NIMS

The National Incident Management System (NIMS) provides a systematic, proactive approach to guide departments and agencies at all levels of government, nongovernmental organizations, and the private sector to work seamlessly to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life and property and harm to the environment.

NIMS is based on the Incident Command System (ICS). ICS is a standardized, on-scene, all-hazards incident management approach that:

- Allows for the integration of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure.
- Enables a coordinated response among various jurisdictions and functional agencies, both public and private.
- Establishes common processes for planning and managing resources.
- Aligns federal, State, and local special-purpose incident management and emergency response plans into an effective and efficient structure.

ICS is flexible and can be used for incidents of any type, scope, and complexity. ICS allows its users to adopt an integrated organizational structure to match the complexities and demands of single or multiple incidents. NIMS works in tandem with the National Response Framework (NRF). NIMS provides the template for the management of incidents, while the NRF provides the structure and mechanisms for national-level policy for incident management.

This Plan format aligns itself with the NRF by incorporating NIMS and employing a functional approach to providing assistance. The SEOP is an ESF structure where emergency functions are assigned to a lead state agency with other departments in supporting roles. The lead or co-lead agencies will work with the DEM in the development, coordination, and maintenance of appropriate annexes and for ensuring tasks are completed during emergency operations.

Public Information Plan

Each co-lead agency has an established public information component process that is relative to their policies and procedures during a normal course of business. During an energy emergency the co-lead agencies will coordinate with DEM with efforts to augment the State's Public Information Plan which resides under ESF #15 External Affairs. The Public Information Strategy for this Plan is included as a communication framework to be applied to all other strategies.

Five Phases of Incident Management

Prevention, Preparedness, Mitigation, Response, and Recovery

Prevention

Prevention means to deter or avoid. Preventative measures taken in advance of an incident reduce or eliminate anticipated impacts. It involves applying intelligence and other information to a range of activities that may include countermeasures as deterrent operations, heightened inspections, improved surveillance and security operations, intervention to stop an incident, investigations to determine full nature and source of the threat, and as appropriate, special law enforcement operations aimed at deterring, preempting, interdicting or disrupting illegal activity and apprehending perpetrators and bringing them to justice.

- **Practices:**
 - Prioritization of sector assets and systems needs to be flexible according to circumstances
 - Information sharing and communication
 - Physical and cyber security
 - Coordination and planning
 - Public confidence
 - CEO in conjunction with PUC, DEM, CDPS-DHS and other state and local government agencies, and with collaboration among the private sector partners
- **Desired Results:**
 - Better understanding of asset risk and vulnerability and necessary protection measures
 - Effective prevention program development
 - Long-term solutions
 - Research and development (R&D).
 - Comprehensive public information

Preparedness

Preparedness infers the state of readiness. It is defined as the range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to and recover from domestic incidents. Preparedness is a continual process involving efforts at all levels of government and between government and private sector and non-governmental organizations to identify threats, determine vulnerabilities and identify required resources.

- **Practices:**
 - Ensure training is relevant to full spectrum of hazards including low frequency/high impact hazards
 - Testing and implementing appropriate technologies that increase effectiveness of response
 - Designing scope of exercises for applicability to a wide range of **realistic** potential hazards
 - Community outreach and education programs about energy disruptions and secondary disaster impacts
- **Desired Results:**
 - Preparedness translates to increased efficiency and efficacy of response
 - Decreases stakeholder losses associated with hazards
 - A proactive comprehensive emergency management program increases stakeholder confidence and encourages investment

Mitigation

Mitigation means to lessen or alleviate. Mitigation measures are implemented in advance of an incident and are usually based on losses experienced from prior events. Mitigation activities provide a critical foundation in the effort to reduce the loss of life and property from natural and/or human-caused disasters by avoiding or lessening the impact of a disaster; and provide value to the public by creating safe communities. Mitigation seeks to alter the cycle of disaster damage, reconstruction and repeated damage and have long-term sustained effects. An effective mitigation strategy will include implementable actions from all phases of incident management.

- **Practices:**
 - Continued high-quality risk and vulnerability assessments, supply chain and interdependency charting, and long-term mitigation benefit/cost analysis
- **Desired Results:**
 - Optimum return on investment per mitigation dollar, decreased recovery time, increased prevention and minimization of hazard impact and damage costs

Response

Response means an elicited reaction to an occurrence. Response encompasses the activities that address the immediate and short-term direct effects of an incident. Actions are intended to save lives, protect property and the environment, and meet basic human needs. It involves the execution of emergency plans that activates a collaborative system in support of short-term recovery and seeks to reduce the probability of secondary impacts.

- **Practices**
 - Cross-sector information gathering and sharing, command and control, and decision-support practices to facilitate prompt and cost-effective response
 - Leveraging technologies to increase pace and efficiency of response
 - Systematically prioritizing response processes to prevent and limit recovery costs
 - Attention to appropriate resource allocation to prevent deployment duplication
- **Desired Results**
 - Prompt and effective response decreases stakeholder losses associated with hazards
 - Cost-effectiveness increases perceived and actual stakeholder return on investment (ROI), and increases relative capabilities of emergency management organizations on per dollar basis

Recovery

Recovery means to recuperate and revitalize. Recovery is the rapid and orderly rehabilitation of victims, the reconstitution of government operations and critical services, and the restoration of institutions to suitable economic stability and confidence. It encompasses activities for both short and long term recovery operations.

- **Practices**
 - Immediate/temporary restoration of lifelines to protect public and critical infrastructure
 - Conducting thorough damage assessments of affected systems prior to recovery resource deployment
 - Strategic recovery resource management and recovery processes to eliminate duplicated efforts, price gouging, and contractor fraud
- **Desired Results**
 - Recovery pre-planning produces higher return on investment per recovery dollar
 - Increases stakeholder confidence and perception of responding organizations' effectiveness

Administration, Logistics, and Mutual Aid

Administration

In the Governor's declaration or Executive Order of Disaster Emergency will state if any normal State administrative procedures will be suspended, modified or made optional in the best interest of emergency operations.

Finance

Financial accountability and resource tracking is imperative during emergency operations. Additional State finance personnel may be requested to assist the Finance Section Chief in the SEOC. ESF#12 financial responsibilities must include the separation of public and private utilities' resources and damage cost assessments. If necessary additional personnel may be assigned to support ESF#12 in maintaining logs, records, receipts, invoices, purchase orders, rental agreements, etc. Accurate documentation of resources must accompany claims, purchases, reimbursements and disbursements. Professional record keeping practices is necessary to facilitate disaster closeouts and be available for post recovery audits.

The Governor may make additional funds available from the Disaster Emergency Fund. If insufficient, the Governor has the authority under a State Declaration of Disaster Emergency to transfer and expend moneys appropriated for other purposes.

State departments, offices and agencies designated as lead agencies for Emergency Support Functions that are actively supporting emergency operations will be responsible for organizing their functional activities to provide financial support for their operations. Each department is responsible for maintaining appropriate documentation to support requests for reimbursement; for submitting bills in a timely fashion, and for closing out assignments.

Logistics

DEM

- Provides logistics for SEOP staff (food, lodging, communications equipment, office supplies, mapping, WebEOC, etc.)
- Utilizing Connect Colorado and the Resource Ordering Status System (ROSS) or other resource database, DEM coordinates resources from a supplying jurisdiction to the requesting jurisdiction.
- Provide staffing for SEOC during activations

CEO

- Provides staffing for continued representation for ESF #12 in the SEOC

PUC

- Provides staffing for continued representation for ESF #12 in the SEOC

Utilities

- Provides logistics for emergency response operations crews
- Provides labor and equipment for recovery operations

Mutual Aid Agreements – State Government

Colorado has an Intergovernmental Agreement for Emergency Management which provides a structure for mutual aid within the State of Colorado.

Compact Agreements

Mutual aid agreements, compacts, and assistance agreements are agreements between agencies, organizations, and jurisdictions that provide a mechanism to quickly obtain emergency assistance in the form of personnel, equipment, materials, and other associated services. The primary objective is to facilitate rapid, short-term deployment of emergency support prior to, during, and after an incident.

Emergency Management Assistance Compact (EMAC)

EMAC offers assistance during governor-declared states of emergency through a responsive, straightforward system that allows states to send personnel, equipment, and commodities to help disaster relief efforts in other states. Through EMAC states can also transfer services, such as shipping newborn blood from a disaster-impacted lab to a lab in another state. The strength of EMAC and the quality that distinguishes it from other plans and compacts lie in its governance structure; its relationship with federal organizations, states, counties, territories, and regions; the willingness of states and response and recovery personnel to deploy; and the ability to move any resource one state wishes to utilize to assist another state. EMAC establishes a firm legal foundation. Once the conditions for providing assistance to a requesting state have been set, the terms constitute a legally binding contractual agreement that makes affected states responsible for reimbursement. The EMAC legislation solves the problems of liability and responsibilities of cost and allows for credentials, licenses, and certifications to be honoured across state lines. Deploying resources through EMAC leverages federal grant dollars invested in state and local emergency management resource capabilities.

Memorandums of Understanding

- DEM maintains an MOU with the American Red Cross
 - This MOU outlines the process for shelter and feeding operations during a disaster event.
- DEM maintains an MOU with the US Air Force

- This MOU outlines the process for procuring the US Air Force for search and rescue operations.
- DEM maintains an MOU with the Federal Emergency Management Agency (FEMA)
 - This MOU outlines the process for federal level emergency assistance.

Mutual Aid Agreements – Utilities

As a rule, some utilities have agreements in place for labor rather than for equipment. The industry's established relationships allows for convenient contracting capabilities on the "fly" if necessary. At times, a handshake still seals the deal.

Regulated and unregulated utilities alike, in Colorado, also have an established relationship with the Western Electricity Coordinating Council (WECC). WECC is the Regional Entity responsible for coordinating and promoting bulk electric system reliability in the Western Interconnection. In addition, WECC provides an environment for coordinating the operating and planning activities of its members as set forth in the WECC Bylaws.

WECC is geographically the largest and most diverse of the eight Regional Entities that have Delegation Agreements with the North American Electric Reliability Corporation (NERC). WECC's service territory extends from Canada to Mexico. It includes the provinces of Alberta and British Columbia, the northern portion of Baja California, Mexico, and all or portions of the 14 Western states. Due to the vastness and diverse characteristics of the region, WECC and its members face unique challenges in coordinating the day-to-day interconnected system operation and the long-range planning needed to provide reliable electric service across nearly 1.8 million square miles.

An important tool for members is the use of WECCnet. It is an internal communication clearing house where members can quickly exchange information continually. Due to their extensive membership, WECC can rapidly correspond with members to facilitate necessary resources during an electric outage or disruption event.

Recovery/Restoration Strategy

The EA Recovery/Restoration Strategy is based on the agreement of the EAAG as a result of the EA planning process relative to the recovery phase of an emergency that has had an energy impact component. There are various energy scenarios that will necessitate recovery and restoration operations from the Division of Emergency Management and their energy sector partners. Some scenarios include:

- **Extended Power Delivery Disruption:** The shortage of any vital resource as a consequence of interruption or shortage of electricity, petroleum products, natural gas, propane gas, or any of the resources used in the generation of electricity.
- **Incoming threats to critical infrastructure** including atmospheric and space weather phenomena may have an extended impact requiring post disaster recovery and restoration operations to regain energy delivery and reliability.
- **Intentional or deliberate act to disrupt power delivery** may necessitate an extended recovery and restoration period to restore critical electric, natural gas, and petroleum infrastructure and to provide resources for victims displaced or without power.

When it is not possible to avert a crisis, it is imperative to take such actions as are necessary to ensure the health, safety, and welfare of the residents of the state. Vital resources are defined to include food and water for domestic use, water for agricultural or industrial use, and water for electric power generation, petroleum based fuels, uranium, coal, natural gas, propane gas, or any other form of energy.

The actions identified in the Recovery/Restoration strategy are primarily electric sector-specific with relative natural gas infrastructure impacts. The updated Liquid Fuels Plan is referenced in the Energy Sector Interdependencies Section and is provided in full in the Appendix.

Purpose

The purpose of this strategy is to provide a framework for smooth operations from immediate lifesaving response activities while recognizing there are simultaneous recovery activities. Although the emphasis on response will diminish while focus on recovery operations will increase, this strategy does not imply that the two operational periods are separate, but is meant to augment one to the other.

Recovery consists of a sequence of short and long term activities both concurrent and interdependent that progressively advances a community back to normal. Within recovery, actions are taken to assist individuals, households, businesses, governmental services, and critical infrastructure to meet basic needs and return the affected communities to an *acceptable* level of self-sufficiency. Acceptability will vary and would be defined based on the specific conditions of the impacts and the magnitude of resources necessary to restore operability of basic services.

Restoration of critical infrastructure and services is one component of recovery operations. In this strategy, restoration of critical electric infrastructure is emphasized since all other sectors depend on the continuity of electric power delivery.

Activating a systematic framework that provides timely and coordinated recovery and restoration activities is vital to the success of incident recovery. The protection of critical infrastructure and the ability to rapidly restore normal commercial activities can quickly mitigate the initial impact of an incident and improve the **short-term** quality of life. Depending on the complexity of the incident, however, recovery efforts may require **long-term** solutions and involve significant contributions from all sectors of society.

Short-term recovery is immediate and overlaps with response. It includes actions such as providing essential public health and safety services, restoring interrupted utility and other essential services, reestablishing transportation routes, and providing food and shelter for those displaced by the incident. Although called “short term,” some of these activities may last for weeks. Recovery from an incident is unique to each community and depends on the nature of damage and the resources available to address it.

Long-term recovery is outside the scope of this Plan and involves concentrated efforts to specific sectors for months or years depending on the severity and extent of the damage sustained. It may involve extensive rehabilitation of personal lives and the restoration of the livelihood of the community. Long-term recovery may include the development, coordination, and execution of site-restoration plans; reestablishment of critical services programs; reconstitution of government operations and services; programs to provide housing and promote restoration; and additional measures to restore social, political, environmental, and economic stability.

Overarching Plan Goals

- 1) Provide Public Safety and Welfare and Protect Critical Infrastructure
- 2) Improve Communication, Coordination, and Public Information
- 3) Expand and Improve Energy Assurance Awareness through Educational Outreach
- 4) Improve Investment for Appropriate Reliability, and Resiliency

Authority

- State
 - Title 24, Article 32, Part 2101 et. Seq., Colorado Revised Statutes, as amended; entitled the *Colorado Disaster Emergency Act of 1992*.
 - Article IV, Constitution of the State of Colorado; entitled the *Executive Department*.
- Federal
 - Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. §§ 5121-5207).

- The National Response Framework, January 2008.
- National Disaster Recovery Framework, September 2011
- Utilities
 - North American Electric Reliability Corporation (NERC)
 - Standards Process Manual (available online at http://www.nerc.com/fileUploads/File/Appendix_3A_Standard_Processes_Manual_Rev%201_20110825.pdf)
 - Reliability Standards <http://www.nerc.com/page.php?cid=2|20>
 - Communications (COM-001 through COM-002)
 - Critical Infrastructure Protection (CIP-001 through CIP-009)
 - Emergency Preparedness and Operations (EOP-001 through EOP-009)
 - EOP-002-2 Capacity and Energy Emergencies – ensures Reliability Coordinators and Balancing Authorities are prepared for capacity and energy emergencies
 - Event Analysis Program (revised February 21, 2012) – analysis of operations, planning and critical infrastructure protection processes

Best Practices

Best practices are considered a method or technique that has consistently shown results superior to those achieved with other means; a benchmark to maintain quality. A "best" practice can evolve or be eliminated as improvements are discovered or as principles are determined non-applicable. The following best practices for the recovery/restoration phase or operational period have been developed based on previous disaster recovery experience.

- Recovery begins with pre-disaster preparedness planning activities
- To begin recovery operations as the immediate imperatives for response are being addressed
- To identify needs and resources for the affected areas
- To coordinate recovery and restoration activities through DEM and the ESF framework
 - Communicate with owner/operators for energy sector critical infrastructure and services restoration information and timeline
 - Report information to SEOC and informational briefings
- Provide financial documentation
- Coordinate public information through a Joint Information System
 - Provide incident assistance programs and fact sheets via websites
- Provide technical assistance for the Disaster Recovery Centers when applicable
- To consider long-term mitigation activities and coordinate with ESF #14
- Assist in transition from State to local disaster recovery operations

Scope

The Recovery Strategy uses an all-hazards approach addressing a full range of complex requirements surrounding recovery and restoration from an energy emergency. It details the specific incident management roles and responsibilities of State departments and agencies as well as the private utilities stakeholders that may be involved in recovery and restoration

operations. It establishes a system for collaborative communication between State government and private utility stakeholders that provide accurate information to the Governor and assists in returning societal functions back to normal.

Planning Situations and Assumptions

Situations

- Electric power restoration may be intermittent, occur slowly and be restored in specific sections of the community depending on damage impact and safety issues
- Temporary and/or alternate transportation routes may affect traffic flow patterns
- Telecommunications capability may be unavailable or intermittent
- Interdependent network systems may be restored in stages impeding continuity of service
- Delays in the production, refining, delivery of petroleum-based products may be extended as a result of commercial electric power restoration delays
- Restoration of an energy system in one geographic region may temporarily supply energy to another region with greater need. Service to normal customer base may be compromised. Consequently, prioritization of critical assets for restoration can affect energy supply and transportation across Intra-State, Inter-State, and/or International regions.
- Quick onset of power restoration can cause increased strain on the electric grid creating potential for secondary impacts and lack of power continuity. Critical services may be further affected.
- Local and State government operations may be requested to prioritize critical functions and allocate resources accordingly
- Potential for other secondary impacts (i.e., fires, hazardous materials, explosions) may be reduced as operations are more focused on recovery activities, but awareness for such should remain high as a precautionary measure for recovery personnel and public safety.
- In an act of terrorism, great potential exists for dangerous diversionary tactics used to impede recovery operations. This would necessitate mobilizing tier 2 response resources further complicating matters.
- The preservation of evidence is critical throughout all phases of a suspected terrorist incident.
- Economic impacts may be realized for an extended period of time requiring economic relief.

Assumptions

- Local, State and Federal government and the private sector share in the responsibility to recover from an energy emergency
- Government must continue to function during recovery operations
- Information sharing must continue to occur during recovery operations between public and private entities and across all levels of government
- Redundant power generation capability and fuel reserves may be required for continuity of critical State and local services for an extended period of time

- Transportation systems (mass transit, traffic lights, etc.) which rely on electric power may not be restored to capacity for an extended period of time causing massive transportation issues.
- Agriculture and Food sector may experience significant delays in supplying life-sustaining resources to an affected area until recovery operations are well established
- Banking and Finance sector communications capabilities may experience intermittent reliability for an extended period of time
- Natural Resources sector may require unique recovery operations for
 - Dams
 - Renewable Energy Operations
 - Fossil Fuels extraction processes

Recovery Function Matrix

During recovery operations, resources are tracked by DEM and other eligible organizations as in the response phase, but financial expenditures for response and recovery are usually documented separately for reimbursement eligibility purposes. In Figure VIII-3, general recovery functions are listed.

Figure VIII-3 General Recovery Matrix (one and two-page view)

GENERAL FUNCTIONS	STATE AGENCIES										ENERGY SECTOR STAKEHOLDERS						NGOs	LOCAL AGENCIES																				
											Electric Utilities		Natural Gas	Liquid																								
											Regulated	Unregulated																										
	Colorado Energy Office	DoLA-Div of Emergency Mgt	DoRA-Public Utilities Commission	Governor's Office of Information Technology	Office of Economic Development	Dept of Public Safety	Dept of Public Health & Environment	Dept of Human Services	Dept of Transportation	Dept of Agriculture	DoLA-Natural Resources	DoLA-Local Government	DoLA-Housing	Dept of Labor-Div of Oil & PS	Dept of Military & Veterans Affairs	Dept of Personnel & Admin	Xcel Energy	Black Hills	TriState	Colorado Rural Electric Assn	Xcel Energy	Black Hills	Colorado Natural Gas	Colorado Oil and Gas Assn	American Red Cross	Salvation Army	Colo Voluntary Org Active in Disaster	local emergency management	local law enforcement	local fire department	local public health	local utilities	local road & bridge	local public works	local environment	local information technology		
Damage Assessment	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
Provide Liason to DEM		x			x	x	x	x	x	x	x	x	x	x	x	x							x	x	x													
Notification and Reporting	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
Information Sharing (collaboration)	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
Recovery Operations Public Information	x	x	x		x																																	
Post Disaster Warning for Secondary Impacts	x	x																																				
Recovery Operations Training	x				x																																	
Mission Tasking/Event Tracking	x																																					
Recovery Operations Personnel Deployment	x																																					
Recovery Operations Resource Mobilization/Management	x																																					
Recovery Operations Financial Tracking/Documentation	x																																					
Damage Assessment Teams (coordination of)	x																																					
Implement Debris Management Plan	x																																					
Mass Care, Housing and Human Services																																						
Extended Sheltering																																						
Mass Feeding																																						
Bulk Distribution (coordination of)																																						
National Guard Recovery Operations	x																																					
Short to Long-Term Housing (not initial sheltering)	x																																					
Public Health and Medical Recovery Operations																																						
Access & Functional Needs Populations Management	x																																					
Public Health (food contamination)																																						
Public Health (mass prophylaxis)																																						
Food Donations and Distribution	x																																					
Animal Recovery Operations																																						
Structural Damage (public protection)																																						
Restoration of Essential Transportation System																																						
Restoration of Essential Utilities Infrastructure																																						
Restoration of Essential Communications Systems																																						
Restoration of Essential Water Systems																																						
Restoration of Essential Wastewater Systems																																						
State Facilities Management																																						
State Recovery Center(s) Mobilization	x																																					
Victim Services																																						
Victims Case Management																																						
Volunteer Management	x																																					
Donations Management																																						
Public Assistance Programs Administration	x																																					
Individual Assistance Programs Administration	x																																					
Economic Impact and Recovery Assessment																																						
Economic Assistance Programs Administration																																						
Environmental Protection (air quality)																																						
Environmental Protection (water quality)																																						
Environmental Protection (soil quality)																																						
Fatality Management	x																																					
Transition Planning	x																																					
Recovery Center Demobilization	x																																					

STATE AGENCIES

- Colorado Energy Office
- DoLA-Div of Emergency Mgt
- DoRA-Public Utilities Commission
- Governor's Office of Information Technology
- Office of Economic Development
- Dept of Public Safety
- Dept of Public Health & Environment
- Dept of Human Services
- Dept of Transportation
- Dept of Agriculture
- Dept of Natural Resources
- DoLA-Local Government
- DoLA-Housing
- Dept of Labor-Div of Oil & PS
- Dept of Military & Veterans Affairs
- Dept of Personnel & Admin

GENERAL FUNCTIONS	Colorado Energy Office	DoLA-Div of Emergency Mgt	DoRA-Public Utilities Commission	Governor's Office of Information Technology	Office of Economic Development	Dept of Public Safety	Dept of Public Health & Environment	Dept of Human Services	Dept of Transportation	Dept of Agriculture	Dept of Natural Resources	DoLA-Local Government	DoLA-Housing	Dept of Labor-Div of Oil & PS	Dept of Military & Veterans Affairs	Dept of Personnel & Admin
Damage Assessment		x	x	x			x	x			x				x	
Provide Liason to DEM			x				x	x	x	x	x	x	x		x	
Notification and Reporting	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x
Information Sharing (collaboration)	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Recovery Operations Public Information	x	x	x		x		x	x								
Post Disaster Warning for Secondary Impacts	x	x					x			x						
Recovery Operations Training		x			x		x	x				x				
Mission Tasking/Event Tracking		x					x	x								
Recovery Operations Personnel Deployment		x					x	x				x				
Recovery Operations Resource Mobilization/Management		x					x	x				x				
Recovery Operations Financial Tracking/Documentation		x					x	x				x	x			
Damage Assessment Teams (coordination of)		x														
Implement Debris Management Plan		x					x			x						
Mass Care, Housing and Human Services							x	x							x	
Extended Sheltering								x							x	
Mass Feeding								x								
Bulk Distribution (coordination of)								x								x
National Guard Recovery Operations		x														x
Short to Long-Term Housing (not initial sheltering)		x						x							x	
Public Health and Medical Recovery Operations								x								
Access & Functional Needs Populations Management		x							x							
Public Health (food contamination)								x								
Public Health (mass prophylaxis)								x								
Food Donations and Distribution		x						x								
Animal Recovery Operations								x								
Structural Damage (public protection)								x								
Restoration of Essential Transportation System																x
Restoration of Essential Utilities Infrastructure			x													x
Restoration of Essential Communications Systems				x												x
Restoration of Essential Water Systems								x								x
Restoration of Essential Wastewater Systems								x								x
State Facilities Management																
State Recovery Center(s) Mobilization		x						x								
Victim Services								x	x							x
Victims Case Management								x	x							x
Volunteer Managemnet		x						x	x							
Donations Management								x	x							
Public Assistance Programs Administration		x							x							
Individual Assistance Programs Administration		x							x							x
Economic Impact and Recovery Assessment			x					x								x
Economic Assistance Programs Administration								x								x
Environmental Protection (air qulaity)									x							
Environmental Protection (water quality)									x							
Environmental Protection (soil quality)									x							
Fatality Management		x							x							
Transition Planning			x						x	x						
Recovery Center Demobilization		x							x	x	x					

Roles and Responsibilities

Introduction

Clarification of primary Energy Sector stakeholders’ roles and responsibilities relative to Recovery and Restoration activities are bulleted in the table below. Clarifying recovery operational processes among stakeholders improves communications and provides opportunity for continued collaboration.

Office of the Governor
<ul style="list-style-type: none"> ✓ Authorized to activate the SEOP under 24-32-2104(5) CRS through the issuance of an Executive Order. <ul style="list-style-type: none"> ○ Appropriate National Guard resources during recovery operations ○ Suspend selected State regulations

Colorado Division of Emergency Management
<ul style="list-style-type: none"> ✓ The State Emergency Operations Center (SEOC) can be activated at any time by the Director of the Division of Emergency Management ✓ The function of the SEOC is to provide assistance to local jurisdictions. This assistance takes the form of: <ul style="list-style-type: none"> ○ Providing Statewide situational awareness ○ Coordinating State, local, Federal and private sector resources that the impacted jurisdiction(s) need to respond and recover from a natural, technological, or human-caused incident. ○ Documenting and routing resource requests ✓ Assist in coordination and information sharing. <ul style="list-style-type: none"> ○ Primary role is to support in-house utility recovery by providing utilities with information and coordination support. ○ Not necessary to have Utility representative at the SEOC, though recommended. WebEOC can be used virtually to input information relative to a disaster event and track its requests, resources, and other critical information. ✓ The SEOP is an ESF structure that is in place to handle energy-related issues. DEM requests State Agency ESF representatives (of the affected sectors) to continue to assist in coordinating recovery operations.

Colorado Energy Office & Public Utilities Commission
(Co-Lead Agencies for ESF#12)

During An Event

- ESF #12 - Energy has a co-lead structure. The Colorado Energy Office (CEO) and the Public Utilities Commission (PUC) will be requested to respond to the State Emergency Operations Center for assistance with response and recovery operations as needed.
- CEO and/or the PUC will implement components of the Colorado Energy Assurance Emergency Plan (CEAEP) as necessary for recovery operations.
 - CEO/PUC coordinates with the Joint Information System during recovery operations as needed.
- ✓ Maintain communication with all energy-related organizations, companies, and special districts during restoration operations to communicate to the SEOC any need for recovery assistance by the State such as debris removal for repair crews. This would be coordinated with other ESF's participating within SEOC.
- ✓ Share responsibilities for the collection and evaluation of information on energy system damage and restoration activities. The term "energy" includes producing, refining, transporting, generating, transmitting, conserving, building, distributing, and maintaining energy systems and system components.
- ✓ May be asked to provide current estimations on the energy sector recovery progress, an anticipated restoration timeframe, areas affected by the disruption, and the percentage or number of residential and business entities without services.
- ✓ Additional personnel may be requested by CEO and the PUC to respond to the field or to the SEOC to assist with gathering current information for support to recovery operations.
- ✓ Assist in tracking information from the utilities' coordination of interstate resources (i.e. equipment from utilities of other regions/states via Mutual Aid Agreements, etc.) that might be utilized for recovery operations.
- ✓ Coordinate with the utilities involved to implement recovery strategies identified in the CEAEP.
- ✓ Provide periodic utility recovery status information during SEOC briefings so that current information on power restoration can be made available to local emergency offices via the WebEOC tool or through the JIS.

Colorado Energy Office & Public Utilities Commission
 (Co-Lead Agencies for ESF #12)
During Normal Operations

- ✓ As co-lead agencies in ESF #12, the CEO and the PUC are required to fulfill the following duties:
 - Provide an Emergency Response Coordinator (ERC), which is the lead agency representative for a specific ESF as outlined in the SEOP.
 - ERC will provide support through staff, technical services, and/or equipment to other ESF lead agencies.
 - Occupy a seat at the SEOC during the Center’s activation.
 - Participate in SEOC exercises and associated training sessions, which may include WebEOC, SEOC management and forms usage, National Incident Management System (NIMS) training such as, Position Specific Command and General Staff training, etc.
 - During periods of non-activation of the SEOC, be aware of on-going incidents and relay applicable information to DEM (i.e., damage of electric transmission lines, power generating plants, transformers, natural gas pipeline, etc; or the correction of false reports in reference to infrastructure damage)
 - Assist in the periodic review and update of the SEOP due to lessons learned and/or new Federal guidance. Updates to the SEOP are conducted after:
 - An actual event in Colorado
 - An event elsewhere that would improve response
 - After exercises where the After Action Report (AAR) indicates corrective action is warranted to improve disaster operations.
 - Assist in pre-planning efforts for anticipated cascading natural hazards (secondary hazard impacts caused by the degradation from the primary hazard event)
 - Be a decision-maker for their respective organization
 - Have knowledge of and work within the NIMS/Incident Command System, to include the Joint Information System.
 - The ERC should have a well established relationship with public and private utilities providers with 24/7 contact information points for secure information exchange, which establishes accurate situational awareness.
- ✓ Collaborate with the utilities or city/county Local Energy Assurance Plan (LEAP) initiatives to participate as “observers” in their disaster scenario exercises where opportunities to provide recommendations and share expectations for integrated communications can occur.
- ✓ Provide cross-training of in-house personnel

Utilities and Western Electricity Coordinating Council (WECC)	
Xcel Energy	<ul style="list-style-type: none"> ✓ Prioritize the critical users ✓ Restore power to the largest numbers and who has been out longest ✓ Identify areas of outage and work to prioritize response/recovery ✓ Contact local Emergency Managers ✓ Handle public information ✓ Report outage of a certain size to the PUC within 1 hour ✓ File their plan with NERC ✓ Provide a secure/redundant in-house EOC ✓ Provide for a secondary EOC at an alternate location
Black Hills Corporation	<ul style="list-style-type: none"> ✓ Track and report outages to WECC within 24 hours ✓ Monitors SCADA, Smart Meters and uses the Outage Management System ✓ Protect the main grid and equipment ✓ Restore power to their own infrastructure ✓ Provide a secure/redundant in-house EOC ✓ Provide for a secondary EOC at an alternate location
Tri-State Generation and Transmission Association	<ul style="list-style-type: none"> ✓ Follow FERC, NERC standards for reporting ✓ Reporting requirements are based on specific situational occurrences ✓ Report outages to WECC, if situation warranted ✓ Contacts local EMs when Tri-State facilities may be or are impacted. <ul style="list-style-type: none"> ▪ Have facilities in four states, one in Westminster, CO ✓ Have capability of coal production
Western Electricity Coordinating Council (WECC)	<ul style="list-style-type: none"> ✓ Maintain a reliable electric power system in the Western Interconnection. (The Western Interconnection stretches from Western Canada south to Baja California in Mexico, reaching eastward over the Rockies to the Great Plains.) ✓ Assure open and non-discriminatory transmission access among Members ✓ Provide a forum for resolving transmission access disputes between Members ✓ Act as a coordinating entity for the entire West Interconnection for activities of regional organizations with responsibilities for reliability and market functions ✓ Develop and adopt reliability, operating and planning standards, criteria and guidelines necessary to maintain the reliable operation of the Western Interconnection's interconnected bulk power system ✓ Certify Grid Operating Entities in the Western Interconnection ✓ Ensure that interconnected bulk electric system reliability assessments are conducted as needed ✓ Implement the Reliability Management System ✓ Implement any enforcement mechanisms ✓ Develop coordinated planning policies and procedures for the Western Interconnection ✓ Review and assess Local Regional Entity planning processes ✓ Notify NERC, FERC, DHS, DOE, and WAPA ✓ Develop, coordinate and promote consistent interregional operating

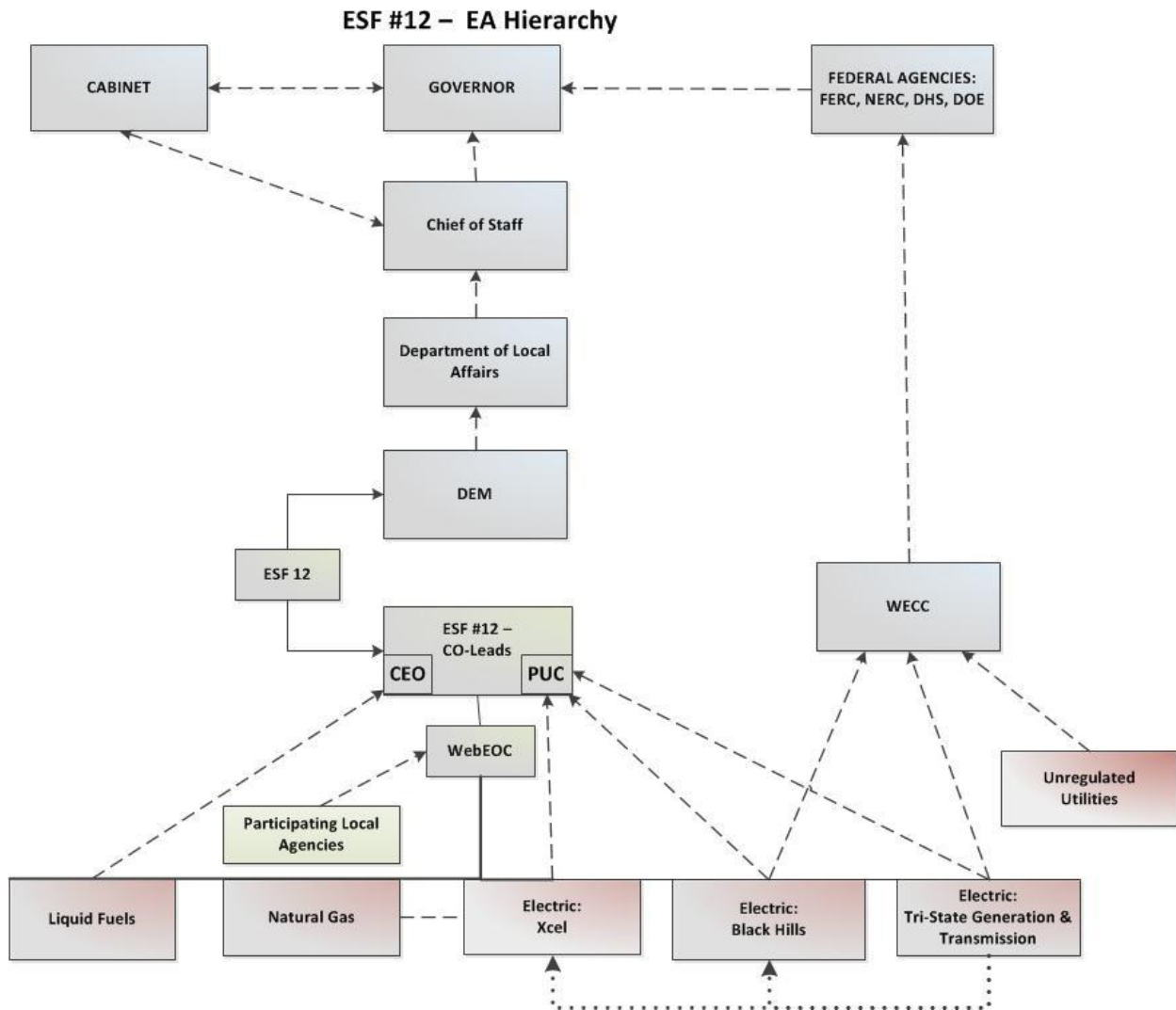
	<p>policies and procedures for the Western Interconnection, consistent with WECC/ERO standards and FERC policy</p> <ul style="list-style-type: none"> ✓ Utilizes WECCnet for internal communications <ul style="list-style-type: none"> ▪ Regulated and non-regulated utilities communicate through WECCnet ✓ Resource dispatch capabilities between members ✓ Conduct annual exercises ✓ Act as the clearing house for outage information
--	--

Colorado Rural Electric Association	
Colorado Rural Electric Association	<p>Colorado’s Rural Electric Cooperatives (REC) purchase power and distribute it to their customers. Generation of power is critical as an external dependency, but not for direct protection by the Cooperatives. The REC’s focus on critical infrastructure lies largely with the transmission and distribution of power to consumers.</p> <ul style="list-style-type: none"> ✓ Assess impact ✓ Conduct Damage Assessment ✓ Repair and/or restore critical infrastructure ✓ Work with Division of Emergency Management on Damage Assessment Cost Analysis

Energy Assurance Emergency Hierarchy-- Recovery/Restoration

During the recovery phase, the standard EA Hierarchy would apply with emphasis on recovery operations specific to the energy sector as a component of overall SEOC Management Operations orchestrated through ESF #12, as shown in Figure VIII-4.

Figure VIII-4 ESF #12 – EA Hierarchy



Continuity of Government

Each level of government should have the capability to preserve, maintain, and reconstitute its ability to carry out essential functions under the threat or actual occurrence of any disaster. Effective and responsive emergency operations are inseparable from the concept of Continuity of Government (COG). The Colorado program identifies two important factors for assuring continuity of government at the local and State level:

- Well defined and understood lines of succession for key officials and authorities
- Preservation of records and critical facilities which are essential to the effective functioning of government and for the protection of rights and interests of the State and its residents

The phases of disaster should not alter continuous attention to the Continuity of Government; however, during the recovery phase or recovery operational period, Government may be in the beginning stages of reestablishment.

State Line of Succession

Article IV of the State Constitution of Colorado, establishes the emergency powers of the Governor and provides for the line of succession in the event the Governor is absent and/or unable to exercise the powers of office.

The legal successor to the Governor is the Lieutenant Governor. The following members (in order of priority) of General Assembly affiliated with the same political party as the Governor follow the state line of succession should the position of Lt. Governor be vacant and/or unable to exercise the powers of office.

- 1) Leader/Speaker of the Senate
- 2) Leader/Speaker of the House of Representatives

http://ballotpedia.org/wiki/index.php/Article_IV,_Colorado_Constitution

- Political subdivisions of the State shall be in accordance with the Constitution.
- State department heads shall designate primary and alternate emergency successors for key supervisory positions.
- Designated interim emergency successors shall be instructed on their responsibilities and the conditions under which they will assume these positions. They shall hold these positions until relieved by the Incumbent or until the emergency or disaster is manageable.

The phases of disaster should not alter continuous attention to State Line of Succession and the Constitutional provisions for such a situation.

Provision of Essential Services

Provision for services that are determined as life sustaining and critical to the immediate economy of the State should have a system in place to maintain or restore such services immediately after a disaster event. Once immediate imperatives of response are being addressed, simultaneous recovery activities should quickly begin to reestablish critical infrastructure sectors that provide essential resources, services or commodities. There are eighteen sectors; energy is one of the eighteen.

Alternative or back-up facility locations should be established in advance to deliver essential services or commodities with consideration for staffing patterns and back-up power generation. Delivery of electric power is essential to the functions of society and, therefore, vital to establish partnership between government and private utilities in advance of an energy emergency.

Each level of government is responsible for sustaining Continuity of Government throughout recovery.

Preservation of Essential Records

Protection of essential State and local records is vital to resume functional operations after a major catastrophe or emergency. There are three categories of essential records and documents that need safeguarding.

- Records that protect the rights and interests of individuals, which include vital statistics, State land and property records, financial and tax records, election records, license registers, articles of incorporation, medical records, etc.
- Records required for effective emergency operations: plans, procedures, and resource inventories; lists of succession - regular and auxiliary personnel; maps, agreements, contracts, and memorandums of understanding.
- Records required to re-establish normal governmental functions and/or to protect the rights and interests of government, which may include federal and State laws, rules and regulations, official proceedings, financial and court records.

Vital records should be duplicated and maintained in the safest, accessible, yet remote location. Reestablishing vital record access is crucial for the economic restoration of an affected community.

Concept of Operations

NIMS

The *National Incident Management System* (NIMS) provides a systematic, proactive approach to guide departments and agencies at all levels of government, nongovernmental organizations, and the private sector to work seamlessly to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life and property and harm to the environment.

NIMS is based on the Incident Command System (ICS). ICS is a standardized, on-scene, all-hazards incident management approach that:

- Allows for the integration of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure.
- Enables a coordinated response among various jurisdictions and functional agencies, both public and private.
- Establishes common processes for planning and managing resources.
- Aligns federal, State, and local special-purpose incident management and emergency response plans into an effective and efficient structure.

ICS is flexible and can be used for incidents of any type, scope, and complexity. ICS allows its users to adopt an integrated organizational structure to match the complexities and demands of single or multiple incidents. NIMS works in tandem with the *National Response Framework*

(NRF). NIMS provides the template for the management of incidents, while the NRF provides the structure and mechanisms for national-level policy for incident management.

This Plan format aligns itself with the NRF by incorporating NIMS and employing a functional approach to providing assistance. The SEOP is an ESF structure where emergency functions are assigned to a lead state agency with other departments in supporting roles. The lead or co-lead agencies will work with the DEM in the development, coordination, and maintenance of appropriate annexes and for ensuring tasks are completed during all phases of an emergency as needed.

Public Information Plan

Each co-lead agency has an established public information component process that is relative to their policies and procedures during a normal course of business. During an energy emergency the co-lead agencies will coordinate with DEM with efforts to augment the State's Public Information Plan which resides under ESF #15 External Affairs. Details for activating the ESF #12 Public Information Plan is included as the final component of the Action Plan Section.

Recovery Phase of Incident Management

Recovery means to recuperate and revitalize. Recovery necessitates rapid and orderly activities taken for the rehabilitation of victims, the reconstitution of government operations and critical services, and the restoration of institutions to suitable economic stability and confidence. It encompasses activities for both short and long term recovery operations. Pre-planning for all phases of an emergency has shown success in reducing the impacts and damage costs of recovering from an incident.

- **Practices**
 - Engage in recovery pre-planning activities
 - Utilize Recovery Support Functions (RSFs)
 - Immediate/temporary restoration of lifelines to protect public and critical infrastructure
 - Conducting thorough damage assessments of affected systems prior to recovery resource deployment
 - Strategic recovery resource management and recovery processes to eliminate duplicated efforts, price gouging, and contractor fraud
- **Desired Results**
 - Recovery pre-planning produces higher return on investment per recovery dollar
 - Increases stakeholder confidence and perception of responding organizations' effectiveness

Administration, Logistics, and Mutual Aid

Administration

In the Governor's declaration or Executive Order of Disaster Emergency it will state if any normal State administrative procedures will be suspended, modified or made optional in the best interest concerning all phases of emergency operations.

Finance

Financial accountability and resource tracking is imperative during all phases of emergency operations. Additional State finance personnel may be requested to assist the Finance Section Chief in the SEOC. ESF#12 financial responsibilities must include the separation of public and private utilities' resources and damage cost assessments. Response and recovery allocated resources are tracked separately to distinguish the impact cost of responding to immediate imperative needs from the cost of resources required in the reestablishment of community. If necessary additional personnel may be assigned to support ESF#12 in maintaining logs, records, receipts, invoices, purchase orders, rental agreements, etc. Accurate documentation of resources must accompany claims, purchases, reimbursements and disbursements. Professional record keeping practices is necessary to facilitate disaster closeouts and be available for post recovery audits.

The Governor may make additional funds available from the Disaster Emergency Fund. If insufficient, the Governor has the authority under a State Declaration of Disaster Emergency to transfer and expend funding appropriated for other purposes.

State departments, offices and agencies designated as lead and co-lead agencies for Emergency Support Functions that are actively supporting emergency operations will be responsible for organizing their functional activities to provide financial support for their operations. Each department is responsible for maintaining appropriate documentation to support requests for reimbursement; for submitting bills in a timely fashion, and for closing out assignments.

Logistics

DEM

- Provides logistics for SEOC staff (food, lodging, communications equipment, office supplies, mapping, WebEOC, etc.)
- Utilizing Connect Colorado and the Resource Ordering Status System (ROSS) or other resource database, DEM coordinates resources from a supplying jurisdiction to the requesting jurisdiction.
- Provide staffing for SEOC during activations
- Provide technical assistance to affected jurisdictions
- Coordinate damage assessment teams

- Administer Public Assistance (PA) programs as needed
- Provide technical assistance to Department of Human Services for Individual Assistance (IA) programs
- GEO
- Provides staffing for continued representation for ESF #12 in the SEOC
- PUC
- Provides staffing for continued representation for ESF #12 in the SEOC
- Utilities
- Provides logistics for emergency response operations crews
- Provides labor and equipment for recovery operations

Mutual Aid Agreements – State Government

Colorado has an Intergovernmental Agreement for Emergency Management which provides a structure for mutual aid within the State of Colorado.

Compact Agreements

Mutual aid agreements, compacts, and assistance agreements are agreements between agencies, organizations, and jurisdictions that provide a mechanism to quickly obtain emergency assistance in the form of personnel, equipment, materials, and other associated services. The primary objective is to facilitate rapid, short-term deployment of emergency support prior to, during, and after an incident.

Emergency Management Assistance Compact (EMAC)

EMAC offers assistance during governor-declared states of emergency through a responsive, straightforward system that allows states to send personnel, equipment, and commodities to help disaster relief efforts in other states. Through EMAC states can also transfer services, such as shipping newborn blood from a disaster-impacted lab to a lab in another state. The strength of EMAC and the quality that distinguishes it from other plans and compacts lie in its governance structure; its relationship with federal organizations, states, counties, territories, and regions; the willingness of states to assist the affected jurisdiction through deployment personnel and equipment; and the ability to mobilize any resource from one state to another for improved operations of large scale emergencies or catastrophic events. EMAC establishes a firm legal foundation. Once the conditions for providing assistance to a requesting state have been set, the terms constitute a legally binding contractual agreement that makes affected states responsible for reimbursement. The EMAC legislation solves the problems of liability and responsibilities of cost and allows for credentials, licenses, and certifications to be honoured across state lines. Deploying resources through EMAC leverages federal grant dollars invested in state and local emergency management resource capabilities.

Recovery Memorandums of Understanding

DEM with the American Red Cross

- This MOU outlines the process for extended shelter and feeding operations between DEM and the American Red Cross.

DEM with FEMA

- DEM maintains an MOU with the Federal Emergency Management Agency (FEMA)
 - This MOU outlines the process for federal level emergency assistance.

Mutual Aid Agreements – Utilities

As a rule, some utilities have agreements in place for labor rather than for equipment. The industry's established relationships allows for convenient contracting capabilities on the "fly" if necessary. At times a hand shake still seals the deal.

Regulated and unregulated utilities alike, in Colorado, also have an established relationship with the Western Electricity Coordinating Council (WECC). WECC is the Regional Entity responsible for coordinating and promoting bulk electric system reliability in the Western Interconnection. In addition, WECC provides an environment for coordinating the operating and planning activities of its members as set forth in the WECC Bylaws.

WECC is geographically the largest and most diverse of the eight Regional Entities that have Delegation Agreements with the North American Electric Reliability Corporation (NERC). WECC's service territory extends from Canada to Mexico. It includes the provinces of Alberta and British Columbia, the northern portion of Baja California, Mexico, and all or portions of the 14 Western states. Due to the vastness and diverse characteristics of the region, WECC and its members face unique challenges in coordinating the day-to-day interconnected system operation and the long-range planning needed to provide reliable electric service across nearly 1.8 million square miles.

An important tool for members is the use of WECCnet. It is an internal communication clearing house where members can quickly exchange information continually. Due to their extensive membership, WECC can rapidly correspond with members to facilitate necessary recovery and restoration resources during an extended electric outage or disruption event.

Mitigation Strategy

Introduction

The definition of mitigation is to lessen or alleviate. Mitigation measures are activities designed to lessen or alleviate potential negative impacts. Depending on the urgency of the mitigation activity, it can be implemented immediately after a disaster occurs in an effort to abate potential secondary impacts and is considered a part of the recovery process; or mitigation measures can be implemented well in advance of an expected future impact and is more associated with preparedness. Either way, mitigation measures are conducted to prevent or reduce the impacts from hazards. Mitigation, though different from all other phases, may be associated with any phase depending on the nature of the activity. Some examples of mitigation activities that are associated with the other phases could include:

In the event of a cyber attack on SCADA, cyber security specialists implement a series of actions to reduce secondary cascade systems failure, but are actually response tactics to lure the hacker back so the perpetrator can be identified and isolated.

- In a flood event, where a channel is significantly eroded requiring a temporary levy to keep a subdivision from further flooding, is a short-term mitigation activity that is part of the recovery process; however, to repair the channel to pre-flood conditions, it may require a long-term construction project with components of design, engineering, and excavation. This is to reduce the impacts of future flood events and considered mitigation, but it improves the capability of preparedness for the next flood event.
- In a geomagnetic storm event, a systems operator upon receiving the warning from the Space Weather Prediction Center, makes a decision to shut down or reroute transmission for a specific area in advance of receiving an expected geomagnetic induced current (GIC) to prevent damage to a large capacity transformer. This is a quick response to an incoming threat, but it lessens or eliminates damage to critical energy infrastructure, thus it would be considered short-term mitigation, but in the response phase of an incoming threat.

Mitigation activities provide a critical foundation in the effort to reduce the loss of life and property from natural and/or human-caused disasters by avoiding or lessening the impact of a disaster; and provide value to the public by creating safe communities. Mitigation seeks to *alter* the cycle of disaster damage, where innovative strategies for reconstruction eliminates or greatly reduces the chance of repeated damage in a future incident and has long-term sustained effects. This is achieved through risk and vulnerability analysis which is the use of advanced technology and engineering to effectively understand the full impact of previous hazards and potential future hazards with the intent to implement actions that address vulnerabilities in a jurisdiction to specific hazard impacts. An effective mitigation strategy should include the identification of goals that are desirable to accomplish based on the risk and vulnerability assessment; objectives to further define steps to accomplish the goals; and implementable action items that will succeed in satisfying the objectives. The EA planning process is a method for data collection and

stakeholder collaboration with the intent to identify areas of strengths and weakness in order to develop a plan for EA improvement. The Mitigation Strategy serves as the potential plan for improvement. The objectives have been identified as *Potential Initiatives* that can be further explored; the action items are identified as *Potential Action Items* that would only be considered for implementation through an energy stakeholder process. The process would be developed by the stakeholders and should include further exploration of the identified issue or capability gap, a benefit/cost analysis for return on investment, and a process to assign responsibility for implementing the action item, if warranted. An effective Mitigation Strategy should include actionable items that address all phases of an emergency.

Addressing mitigation for energy specific emergencies requires similar investment in basic best practices where the outcome has the highest return on investment. In this Mitigation Strategy, four overarching goals were identified for improved energy assurance. All identified capability gaps were considered and potential solutions suggested. The table at the end of this section details the *Potential Initiatives* and *Potential Action Items* that could be implemented with appropriate resources and funding. The rate of success in accomplishing of any one of these items is dependent upon many factors. Providing a forum for continued collaboration to approach these items systematically, such as through the EAAG, is a basic best practice, but cannot ensure ultimate success of any.

Purpose

The Mitigation Strategy differs from the other strategies in that it shifts focus from “what is being done” to “what is going to be done.” Developing a mitigation strategy is a specific planning method of its own. It is a comprehensive effort to analyze the risk and vulnerability assessment data and determine the best actions that can be implemented to reduce or eliminate future impact. Some mitigation projects can take years to complete, but it is an advanced sequence of activities both concurrent and interdependent that progressively advances a community to complete restoration. The implementation of a mitigation strategy is the final phase of the recovery continuum that can bring about a sense of closure to the disaster that has occurred and gives hope for future community protection and safety. The purpose of this Mitigation Strategy is to identify only potential initiatives and potential actionable items that could be further explored for implementation probability. It is encouraged that these initiatives and actions be taken into consideration for future energy assurance improvement.

There are two stages of mitigation: Short-Term Mitigation and Long-Term Mitigation, and two types of mitigation activities: Structural and Non-Structural.

Short-Term Mitigation: Short-Term Mitigation activities may include immediate actions to abate secondary impacts, such as relocating buried lines for channel stabilization or assessing and servicing back-up generations fuel supply for anticipated extended use. These activities can be completed in a relatively short period of time and do not require a considerable amount of planning or design.

Long-Term Mitigation: Long-Term Mitigation activities include following precise methods of operation to evaluate the resources needed to reconstruct any damaged or lost constituent of society. These activities will normally require months or years to complete.

Structural: Structural mitigation refers to any physical construction to reduce or avoid possible impacts of hazards, which include engineering measures and construction of hazard-resistant and/or protective structures and infrastructure. It is a science requiring the expertise of civil engineering, electrical engineering, computer science engineering and design for both new structures and networks and the retrofitting of aged structures and networks.

Non-Structural: Non-Structural mitigation refers to applying, modifying, enhancing, or improving:

- Legislation, statutes, policies, plans, regulations, and/or codes;
- The level of awareness, the development of knowledge, and public information;
- Public/private commitment, methods and/or operating practices which include types of participatory mechanisms (such as memorandums of agreement, intergovernmental agreements, and public/private contracts) and the provisions therein for information sharing that can assist in reducing risk with related impacts.

Scope

The Mitigation Strategy uses an all-hazard, whole community approach addressing a full range of complex requirements surrounding reconstruction and restoration of community where the energy sector has been impacted. It lists potential initiatives and actionable items that could be short and/or long-term mitigation activities. Roles and responsibilities relative to implementing a mitigation strategy can vary considerably from the roles and responsibilities relative to response and recovery. State agencies and departments may play a large role in the reconstitution of government services in jurisdictions that have been severely compromised from disaster. Continuity of such services is reliant upon the restoration of critical infrastructure, in this case, the energy sector critical power delivery systems.

Public and private utilities organizationally respond to an outage in a similar manner, however, public utilities can receive federal reimbursement if they meet the criteria for reimbursement; where private utilities cannot recover expenses through federal assistance. Expedient restoration of electric and natural gas power delivery infrastructure is dependent upon the capability of the utility owner and the magnitude of the disaster. The EA process offers a platform to streamline operations between utilities and the State when the energy sector has been impacted.

ESF #14 in the SEOP is Long-Term Community Recovery, which provides for coordinated measures and policies designed to facilitate recovery. It also provides for effective utilization of resources and a mechanism to stabilize economies and reduce or eliminate future risk. ESF #14 coordinates the damage assessment process and provides government conduit and administrative

means for appropriate assistance during the recovery and mitigation phases. Appropriate assistance for recovery and mitigation activities is normally received in the form of grant funding depending on damage assessment criteria and specific jurisdiction compliance with regulations associated with such funding. In the event that a jurisdiction required significant energy infrastructure reconstruction, utilities representatives may be asked to participate in an ESF #14 Long-Term Recovery or Mitigation Task Force. Currently, under development is a State – level Recovery Plan which is a reflection of the National Disaster Recovery Plan. It is envisioned that the Recovery Plan will realign responsibilities within ESF #14.

Authority

Legal authorities provide the federal government the mechanism to support local and state governments financially after presidential declarations. It allows the federal government to open up monies for communities which have been affected in the presidential declaration to mitigate their impacts.

- State
 - Title 24, Article 32, Part 2101 et. Seq., Colorado Revised Statutes, as amended; entitled the *Colorado Disaster Emergency Act of 1992*.
 - Article IV, Constitution of the State of Colorado; entitled the *Executive Department*.
- Federal
 - Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. §§ 5121-5207).
 - The National Response Framework, January 2008.
- Utilities
 - North American Electric Reliability Corporation (NERC)
 - Standards Process Manual (available online at http://www.nerc.com/fileUploads/File/Appendix_3A_Standard_Processes_Manual_Rev%201_20110825.pdf)
 - Reliability Standards <http://www.nerc.com/page.php?cid=2|20>
 - Protection and Control (PRC-001-1 through PRC-004-WECC-1)

Planning Situations and Assumptions

Planning situations and assumptions during the mitigation phase can be very diverse and dissimilar from those of response and recovery. The situations below are only examples of catastrophic impact that a damage assessment process might reveal and thus require short and long-term mitigation activities and projects.

Situation Examples Requiring Long-Term Community Recovery and Mitigation Activities

- Major reconstruction of electric power infrastructure requiring long-range planning, engineering, design, and construction necessitating alternative short-term power delivery solutions.

- Extended electric power outage to transportation management systems, such as, traffic lights and mass transit systems that rely on electric power for operation.
- Electric powered telecommunications capability incapacitation across multiple jurisdictions. This may necessitate short-term mitigation activities to reinstate some level of communications. This is a mitigation activity applied during the recovery phase, while long-term mitigation solutions are being explored. Once appropriate activities are selected for long-term benefits, then long-term mitigation projects can be designed, engineered and implemented. Alternative means of public information dissemination may be required.
- Interdependent network systems may require extended back-up power generation and may reduce functionality degrading continuity of service. Network engineers may be required to redesign systems on a large scale.
- Delays in the production, refining, delivery of petroleum-based products may be extended as a result of commercial electric power restoration delays requiring short and long term mitigation planning.
- Coordination and participation in short and long-term mitigation task force teams may be required of Federal, State and local government agencies.
- Quick onset of power restoration can increase strain on the electric grid creating potential for secondary impacts and lack of power continuity. Critical services may be further affected during long-term reconstruction activities.

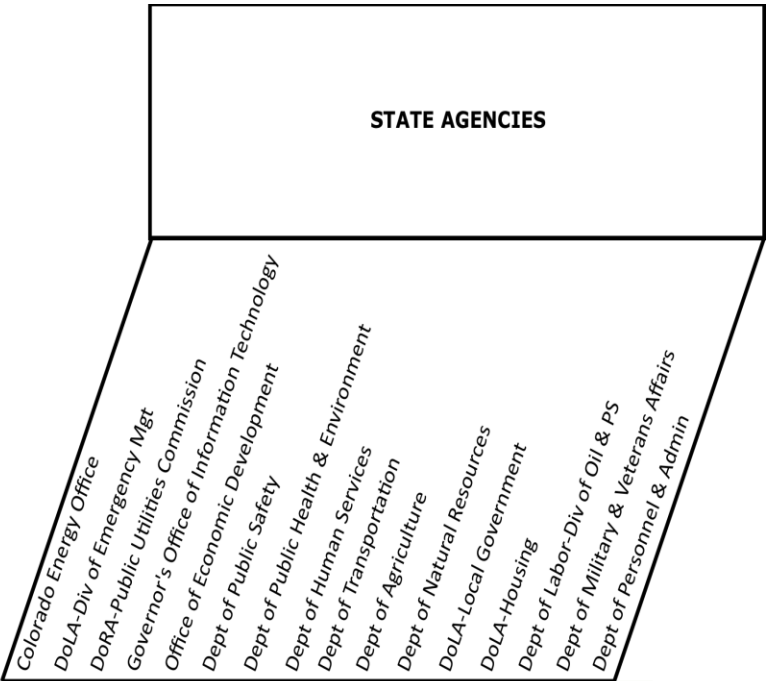
Assumptions

- Short-term mitigation opportunities will be identified during the response phase of an incident.
- Continuity of Government will require temporary operations in remote locations until reconstruction of permanent government offices can be completed.
- Redundant power generation capability and fuel reserves will be required for an extended period of time.
- Agriculture and Food sector impacts from an energy emergency will require special consideration for assistance.
- Banking and Finance sector will be disrupted significantly which will require reestablishment.
- Natural Resources sector will require large-scale mitigation project management orchestrated through Federal government programs, such as the Army Corps of Engineers
- Military Installations without independent power will require special situational awareness and collaboration with utility providers
- Certain hazards will result in higher absenteeism for utility employees. This will in turn affect restoration times.

Mitigation Function Matrix

In the case of a disaster with serious or extreme damage impacts to energy infrastructure and associated infrastructure damages, a Long-Term Community Recovery and Mitigation Task Force would be organized to assess the different long-term recovery and mitigation projects needed to reconstruct the jurisdiction(s). Figure VIII-5 shows the functions associated with such recovery and mitigation needs.

This Page Intentionally Left Blank



Main Functions	Colorado Energy Office	DoLA-Div of Emergency Mgt	DoRA-Public Utilities Commission	Governor's Office of Information Technology	Office of Economic Development	Dept of Public Safety	Dept of Public Health & Environment	Dept of Human Services	Dept of Transportation	Dept of Agriculture	DoLA-Natural Resources	DoLA-Local Government	DoLA-Housing	Dept of Labor-Div of Oil & PS	Dept of Military & Veterans Affairs	Dept of Personnel & Admin
Establish Long-Term Recovery and Mitigation Task Force		X			X		X	X				X	X			
Develop Memorandums of Understanding	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X
Volunteer and Donations Management Tracking		X				X	X									
Establish Long-Term Disaster Recovery Centers		X			X	X					X	X				
Establish Alternative Power Delivery Strategies	X		X		X											X
Back-up Power Generation Procurement	X	X	X		X											X
Long-Term Health and Medical Services Strategies																
Develop Long-Term Housing Strategies		X					X				X	X				
Victim Case Tracking						X	X				X	X				
Displacement of At-Risk Populations							X									
Develop Food Distribution Services						X	X									
Water/Waste Water Quality Issues						X										
Air Quality Issues						X										
Communications and IT Capabilities Reestablishment				X												
Banking and Finance Systems Reestablishment				X							X	X				
Collaborate with State Animal Rescue Team (SART)		X			X		X		X	X						
Debris Management		X			X	X		X								
Resource Management		X			X		X	X								
Conduct Risk and Vulnerability Assessment		X			X	X	X				X	X				
Identify Potential Mitigation Projects		X									X	X				
Identify Mitigation Project Funding Sources		X									X	X				
Consider Critical Infrastructure Protection Strategies	X	X	X	X	X	X										
Consider Economic Redevelopment Strategies	X		X		X						X	X				
Implement Appropriate EA Mitigation Action Items	X		X		X		X									
Consider Impact Reduction Strategies	X	X	X	X	X	X					X	X				
Provide Assistance with Debris Management Plan		X				X										
Collaborate with Colorado Volunteers Org. Active in Disaster		X														
Potential Policy Revision Opportunities	X	X	X		X		X	X	X		X	X	X			
Potential Code/Regulation Revision Opportunities	X		X	X		X	X	X	X		X	X	X			
Financial Management	X	X	X								X	X				

ENERGY SECTOR STAKEHOLDERS										NGOs			LOCAL AGENCIES						
Electric Utilities					Natural Gas			Liquid											
Regulated		Unregulated																	
Xcel Energy	Black Hills	TriState	Colorado Rural Electric Assn	Xcel Energy	Black Hills	Colorado Natural Gas	Colorado Oil and Gas Assn	American Red Cross	Salvation Army	Colo Voluntary Org	Active in Disaster	local emergency management	local law enforcement	local fire department	local emergency medical or public health	local road & bridge	local public works	local environment	local information technology Agency/Company
X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
										X	X	X							
										X	X	X							
										X	X	X							
X	X	X	X	X	X	X	X	X						X					
X	X	X	X	X	X	X	X	X						X					
									X		X								
									X		X								
X	X	X	X	X	X	X	X	X	X	X	X	X	X						
									X	X	X								
									X	X	X								
X	X	X	X	X	X	X	X	X	X										
X	X	X	X	X	X	X	X	X	X										
X	X	X	X	X	X	X	X	X											
X	X	X	X	X	X	X	X	X											
X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
X	X	X	X	X	X	X	X												

Roles and Responsibilities

During the mitigation phase of an incident, State agencies are involved in the reconstruction of a jurisdiction. ESF's are not utilized and the SEOP is not activated for mitigation efforts; therefore, the standard roles and responsibilities cited in the Response and Recovery Strategies are non-applicable here and have been removed. The process for establishing a Long-Term Recovery and Mitigation Task Force is described below.

Office of the Governor
Disaster Declaration

Colorado Division of Emergency Management
<i>Colorado Recovery and Mitigation Task Force</i>
<p>Upon declaration of a disaster by the Governor, the Division of Emergency Management will convene a State Long-Term Recovery and Mitigation Task Force to guide and coordinate State-level recovery actions, including:</p> <ul style="list-style-type: none"> ✓ Establishment of a communication process with recovery officials from affected jurisdictions to ensure Task Force members remain informed about community impacts and needs for State assistance ✓ Preparation of a State-level strategy for applying technical and financial assistance to support local/tribal recovery goals and priorities, using a collaborative, consensus-based process ✓ Coordination of federal and other funding streams for recovery efforts and facilitation of solutions to identified gaps and overlaps in assistance ✓ Establishment of State recovery goals, priorities and milestones, including relevant recovery progress measures, and a process for communicating needed adjustments and improvements to State leadership and stakeholders

**Colorado Energy Office & Public Utilities Commission
(Co-Lead Agencies for ESF #12)**

- ✓ ESF #12 - Energy has a co-lead structure. The Colorado Energy Office (CEO) and the Public Utilities Commission (PUC) will be invited to participate in the Colorado Recovery and Mitigation Task Force, if applicable.
- ✓ CEO and/or the PUC will implement components of the Colorado Energy Assurance Emergency Plan (CEAEP) as necessary for recovery and mitigation operations.
 - CEO/PUC coordinates with the Joint Information System during recovery operations, as needed, and mitigation operations, if applicable.
- ✓ Maintain communication with all energy-related organizations, companies, and special districts during restoration operations to communicate to the SEOC any need for recovery assistance by the State such as debris removal for repair crews. This would be coordinated with other ESF's participating within SEOC.
- ✓ Share responsibilities for the collection and evaluation of information on energy system damage, restoration activities, and potential mitigation strategies. The term "energy" includes producing, refining, transporting, generating, transmitting, conserving, building, distributing, and maintaining energy systems and system components.
- ✓ May be asked to provide current estimations on the energy sector recovery progress, an anticipated restoration timeframe, areas affected by the disruption, the percentage or number of residential and business entities without services, and potential mitigation strategies.
- ✓ Additional personnel may be requested by CEO and the PUC to respond to the field or to the SEOC to assist with gathering current information for support to recovery and mitigation operations.
- ✓ Assist in tracking information from the utilities' coordination of interstate resources (i.e. equipment from utilities of other regions/states via Mutual Aid Agreements, etc.) that might be utilized for recovery and mitigation operations.
- ✓ Coordinate with the utilities involved to evaluate the implementation of recovery and mitigation strategies identified in the CEAEP.
- ✓ Provide periodic utility recovery and mitigation operations status information during SEOC briefings so that current information on power restoration progress can be made available to local emergency offices via the WebEOC tool or through the JIS.

Utilities and Western Electricity Coordinating Council (WECC)

Xcel Energy

Electric Supply:

- ✓ After a disaster event that caused any outage, electric distribution and transmission send out emergency responders and assessors to assess damage and institute the restoration procedures as soon as it is safe to do so.
- ✓ Department Directors will institute alerts and situation room discussions to share information with affected departments, internally, including Customer Care, Media Relations and Corporate Communications.
- ✓ Company’s website and social media accounts will be updated with current information and Customer Call Centers will be sent current updates for customers.
- ✓ Area Managers will receive information to share with the various local authorities affected by loss of service.
- ✓ Regulatory reporting will be accomplished as needed.
- ✓ An appropriate company representative will be sent to the state EOC to serve as a liaison for the public sector. Information on critical needs will be communicated back to the various Control Centers directing restoration efforts from our liaison.
- ✓ Additional supplies and skilled workers will be gathered from other operating companies in Xcel Energy, utility mutual aid agreements and contractors as needed for the restoration effort.
- ✓ Through internal emergency communications tool, Mission Mode, periodic updates will be held and communications will be updated to all areas throughout the restoration process.
- ✓ Public Safety messages will be forwarded to media outlets to assist with safety during the restoration process.
- ✓ Our Media Relations representatives will be working with PIOs for consistent messages.

Gas Supply:

- ✓ Gas distribution and transmission impact - send out emergency responders/assessors to assess damage and institute restoration procedures as soon as safe to do so. Response to fire departments would occur to isolate and mitigate damaged gas systems and to prevent fires.
- ✓ Department Directors will institute alerts and situation room discussions to share information with affected departments, internally, including Customer Care, Media Relations and Corporate Communications.
- ✓ The company website and social media accounts will be updated with current information, and Customer Call Centers will be sent current updates for customers.
- ✓ Area Managers will receive information to share with the various local authorities affected by loss of service.
- ✓ Regulatory reporting will be accomplished as needed.
- ✓ An appropriate company representative will be sent to the state EOC, during activation, to serve as a liaison for the public sector. Information on critical needs will be communicated back to the various Control Centers directing restoration efforts from our liaison.

	<ul style="list-style-type: none"> ✓ Additional supplies and skilled workers are gathered from other operating companies in Xcel Energy, utility mutual aid agreements and contractors as needed for the restoration effort. Large gas outages require shut offs of individual customer meters and special trained professionals to investigate the house, turn on the meter, if it is safe to do so and relight gas appliances. ✓ Through our internal emergency communications tool, Mission Mode, periodic updates will be held and communications will be updated to all areas throughout the restoration process. ✓ Public Safety messages will be forwarded to media outlets to assist with safety during the restoration process. ✓ Our Media Relations representatives will be working with PIOs for consistent messaging. ✓ Large gas outages, because of the public safety issues, require longer to mitigate.
<p>Black Hills Corporation</p>	<p>Transmission and Distribution Response:</p> <ul style="list-style-type: none"> ✓ Actual switching and energization controlled through the Reliability Center ✓ The Reliability Center has disaster plans for internal issues, which include required redundancy ✓ Contingency planning for major black outs (state and regional) and bulk transmission outages are coordinated through the WECC subject to FERC/NERC audit <p>Disaster involving Transmission and Distribution assets:</p> <ol style="list-style-type: none"> 1) Emergency response to damaged lines and equipment <ol style="list-style-type: none"> a. <ul style="list-style-type: none"> ✓ Existing Emergency Plan is executed ✓ As is practical, immediate system repairs or reconfigurations are made by first responders to restore as many services as possible ✓ Efforts are usually prioritized based on life & safety (hospitals, etc.); large industrial, commercial, and institutional (economic and community services); and residential and agricultural ✓ Efforts are coordinated with local and State EOC's b. <ul style="list-style-type: none"> ✓ Outside resources are brought in as required to assist with first response ✓ Includes contractors, sister operating units, and neighboring utilities via mutual aid agreements 2) Plans are begun in parallel with first response to effect major repairs along same priority as first response <ol style="list-style-type: none"> a. <ul style="list-style-type: none"> ✓ Existing material and equipment stockpiles are analyzed against requirements ✓ Crews, equipment, and materials are dispatched as available to begin repair and replacement

	<ul style="list-style-type: none"> b. <ul style="list-style-type: none"> ✓ Engineering and Procurement develop needs assessment for additional supplies, equipment, and services c. <ul style="list-style-type: none"> ✓ Vendors are identified and contacted ✓ Necessary requisitions are expedited d. <ul style="list-style-type: none"> ✓ Company Standards are used to replace critical system components required to restore all customers <p>3) Intermediate and long range replacement and reinforcement of damaged but serviceable infrastructure is coordinated via the engineering and budget process</p>
<p>Tri-State Generation and Transmission Association</p>	<ul style="list-style-type: none"> ✓ Restore Tri-State’s assets ✓ Transmission Maintenance crews respond to reported electrical outages from our rural electric cooperative members. ✓ Repair transmission towers and lines. ✓ Damaged power plants would be making the necessary repairs to restore power generation. ✓ May request or provide assistance from/to members and other utilities depending on the damage impact. ✓ Utilities will share inventory and labor during these situations. ✓ The Tri-State Crisis Management Team would be activated and stay in communication with local and state emergency management officials, members, and other utilities to coordinate these efforts.
<p>Western Electricity Coordinating Council (WECC)</p>	<ul style="list-style-type: none"> ✓ Contact any other utilities in the region that may be affected by the outage ✓ If the outage is large enough conduct a conference call ✓ Based on size of outage additional personnel will be called in <ul style="list-style-type: none"> •Parallel action: Management contacts WECC Communications Director to advise of outage ✓ Contact affected utility again and discuss ongoing mitigation ✓ Discuss progress and any assistance needed from WECC or any other outside entity <ul style="list-style-type: none"> •Parallel action: If a very large outage or infrastructure damage, FERC "Standards of Conduct" will be suspended to allow utilities to share information from their Reliability Side with their Market side to assist in restoration ✓ If outage covers more than one entity, coordinate the recovery from the event <ul style="list-style-type: none"> • Parallel action: Conference with other RC office (one in Loveland, one in Vancouver) and discuss outage and mitigation strategy ✓ Keep all neighboring utilities updated on progress and solicit help for affected utilities <ul style="list-style-type: none"> •Parallel action: May “Direct” entity to shed load to recover from a smaller event as NERC defines recovery periods for smaller outages ranging from 15 minutes to 30 minutes. In the case of a large event, will announce the resumption of normal operations, the re-

	<p>instatement of the "Standards of Conduct" and resumption of Market activities</p> <ul style="list-style-type: none"> ✓ Keep all entities updated on status of the event <ul style="list-style-type: none"> • Depending on the event, NERC Guidelines are to be followed for requesting "Emergency Assistance" or declaring an Energy Emergency for the affected utility. WECC helps to request this "Emergency Assistance" or declare the Energy Emergency for the Utilities ✓ Continue to monitor recovery/restoration and mitigation efforts ✓ Disseminate information on the event to all affected utilities ✓ In a very large event, coordinate to recover to normal ✓ Restoration of load will be coordinated through the WECC RC (Not what load, but when it can be re-connected). ✓ If an Island situation, utility is disconnected from the rest of WECC ✓ Will coordinate the re-synchronization of islands ✓ When System is back to normal the WECC RC will notify all entities of the status of the system ✓ In the case of a large event, will announce the resumption of normal operations, the re-instatement of the "Standards of Conduct" and resumption of Market activities
--	---

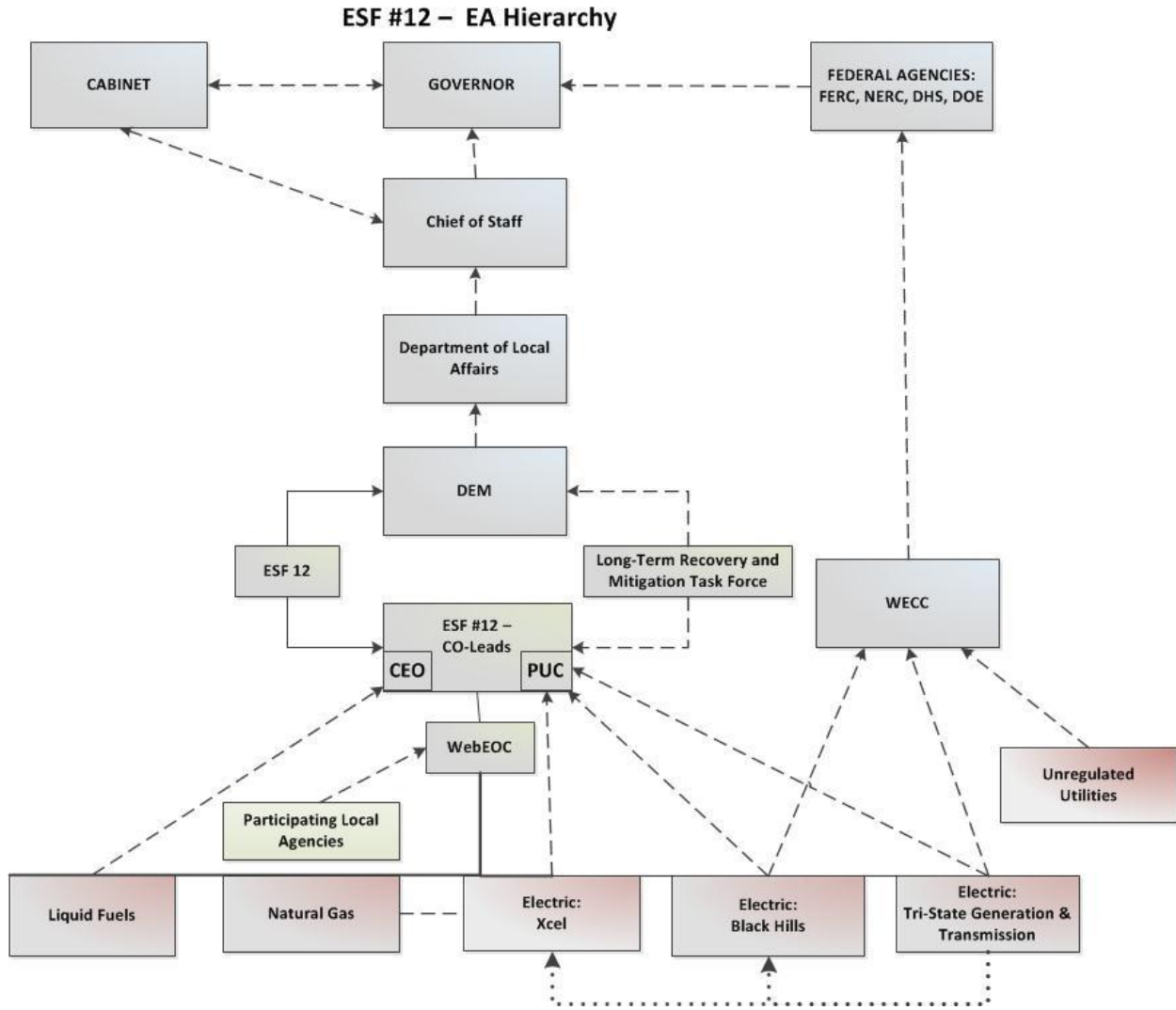
Colorado Rural Electric Association	
Colorado Rural Electric Association	<p>Colorado’s Rural Electric Cooperatives (REC) purchase power and distribute it to their customers. Generation of power is critical as an external dependency, but not for direct protection by the Cooperatives. The REC’s focus on critical infrastructure lies largely with the transmission and distribution of power to consumers.</p> <ul style="list-style-type: none"> ✓ Assess impact ✓ Conduct Damage Assessment ✓ Repair and/or restore critical infrastructure ✓ Collaborate with Division of Emergency Management on Damage Assessment Cost Analysis ✓ Evaluate role in Long-Term Recovery and Mitigation Task Force

Energy Assurance Hierarchy

Mitigation activities conducted during Long-Term Community Recovery are normally implemented through the establishment of a Long-Term Community Recovery and Mitigation Task Force as described above. Under these circumstances, appropriate State agencies are brought together to evaluate and analyze the impact and damage assessment. Their purpose is to identify and utilize adequate resources to further assist a community or jurisdiction reestablish its socio-economic and political stability. The resources are many times linked to a specific grant funding source. The standard EA Emergency Hierarchy would not be applicable to the mitigation phase; however, continued collaboration between these entities is crucial throughout

the reconstruction process. It is shown here to depict collaboration between energy stakeholders and does not indicate that the SEOP or SEOC has been activated.

Figure VIII-6 Energy Assurance Hierarchy



Concept of Operations

NIMS

The *National Incident Management System* (NIMS) provides a systematic, proactive approach to guide departments and agencies at all levels of government, nongovernmental organizations, and the private sector to work seamlessly to prevent, protect against, respond to, recover from, and mitigate the effects from hazardous events, regardless of cause, size, location, or complexity, in order to reduce the loss of life and property and harm to the environment. Utilization of NIMS throughout long-term community recovery can provide structure to the projects and programs implemented and managed.

- Allows for the integration of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure.
- Enables a coordinated response among various jurisdictions and functional agencies, both public and private.
- Establishes common processes for planning and managing resources.
- Aligns federal, State, and local special-purpose incident management.
- Allows the scaling up and/or scaling down of responses depending on situational needs.

ICS is flexible and can be used for incidents of any type, scope, and complexity. ICS allows its users to adopt an integrated organizational structure to match the complexities and demands of single or multiple incidents. NIMS works in tandem with the *National Response Framework* (NRF). NIMS provides the template for the management of incidents, while the NRF provides the structure and mechanisms for national-level policy for incident management.

This Plan format aligns itself with the NRF by incorporating NIMS and employing a functional approach to providing assistance. The SEOP is an ESF structure where emergency functions are assigned to a lead state agency with other departments in supporting roles. The lead or co-lead agencies will work with the DEM in the development, coordination, and maintenance of appropriate annexes and for ensuring tasks are completed during all phases of an emergency as needed.

ESF #14 Long-Term Community Recovery

Transitioning operations to ESF #14 for Long Term Community Recovery does not require the SEOC to remain activated and does not function under SEOC management. ESF #14 has established processes identified in the SEOP that facilitate, coordinate and manage specific activities required establishing long-term recovery teams or a mitigation task force, oversee volunteer and donations management, and implement grant funded mitigation projects. It has the flexibility to operate in an autonomous manner while coordinating with other State agencies and invested stakeholders on behalf of the affected community. Authorized projects are managed to completion or transitioned to appropriate State agencies or back to the local entity once stability is established.

Public Information Plan

Each co-lead agency has an established public information component process that is relative to their policies and procedures during a normal course of business. During an energy emergency the co-lead agencies will coordinate with DEM with efforts to augment the State’s Public Information Plan which resides under ESF #15 External Affairs. Details for activating the ESF #12 Public Information Strategy is included as the final component of this section.

The dissemination of information on short and long-term mitigation activities to the public may be transitioned to the organization or State agency responsible for the implementation of that activity or project.

Mitigation Phase

Practices:

- Continued high-quality risk and vulnerability assessments, supply chain and interdependency charting, long-term mitigation benefit/cost analysis, and feasible investment analysis

Desired Results:

- Optimum return on investment per mitigation dollar, decreased recovery time, increased prevention and minimization of hazard impact and damage costs in future incidents

Figure VIII-7 Tornado in Winsor Colorado, May 25, 2008 – Recovery and Mitigation



<http://www.bing.com/images/search?q=pictures+of+windsor+tornado%2c+colorado&qvvt=pictures+of+windsor+tornado%2c+colorado&FORM=IGRE#x0y2831>

Mitigation Action Plan

Any pre-planning activity with the intent to improve capability could be considered as a mitigation strategy. There are no hard lines of division between the phases of disaster management and many actions can support all five phases simultaneously. Such as, in the case of a cyber security breach, phases of disaster management may not follow a normal pattern or may be indistinguishable altogether. Response tactics may be so technical or clandestine that what appears to be monitoring may in fact be a decoy strategy to expose the intruder. This type of strategic warfare may not be categorized easily where others may be quite evident.

Therefore, the overarching goals of the Plan are well designed to umbrella the many complex components that could be considered for improving energy assurance.

The Potential Initiatives and Potential Action Items are intended to serve as a catalog of issues that could be further explored to better understand their place in improving energy assurance. Since a previous EA Action Plan has not been established by the State and an in-depth benefit/cost analysis on any actionable item has not been conducted, the following list of potential solutions to address the capability gaps presented herein should be considered the results of an identification process only and an opportunity to expand collaboration among stakeholders. Due to the uncertainty of continued EA funding and other financial restrictions, it cannot be stated whether any of the following objectives and action items will be implemented within a certain timeframe. The EAAG will continue to meet on a quarterly basis for monitoring, updating and maintaining the accuracy of the Plan.

Overarching Plan Goals

- 1) Provide Public Welfare and Protect Critical Infrastructure
- 2) Improve Communication, Coordination, and Public Information
- 3) Expand and Improve Energy Assurance Awareness through Educational Outreach
- 4) Improve Investment for Appropriate Reliability, and Resilience

Figure VIII-8 Long-Term Community Recovery and Mitigation Activities: Recovery and Mitigation Planning (left); DEM Donations Management (right)



<http://www.bing.com/images/search?q=pictures-of+windsor+tornado%2c+colorado&qv=pictures-of+windsor+tornado%2c+colorado&FORM=IGRE#x0y1520>

EA Goals, Potential Initiatives and Action Items

Table VIII-1 was developed by the EAAG as part of finalizing the EA process. The x's in the columns indicate the phase of emergency management which that potential initiative addresses. Potential Action Items under that Initiative would also address the same phases so are not repetitively marked.

Table VIII-1 Energy Assurance Goals and Initiatives

Goal 1: Provide Public Welfare and Protect Critical Infrastructure				
<i>The Potential Initiatives and Potential Action Items included in this table are suggested possible solutions that address many of the capability gaps identified. The Capability Gap Analysis and potential Mitigation Strategy is an identification process only and does not bind any individual agency or utility to the responsibility of implementing any one of the items listed, but encourages continued participation in the EAAG, where energy stakeholders can further investigate processes to approach each item methodically.</i>				
Potential Initiative	Preparedness	Response	Recovery / Restoration	Mitigation / Prevention
1.1 Coordinate for response protocol with cyber security department/ team/ agency	x	x		
1.2 Develop cyber security working group	x	x	x	x
1.3 Mitigation measures against cyber attack	x	x	x	x
Potential Action Items: Tier 1				
1.3.1 Build cyber defense in layers				
1.3.2 Apply authentication process				
1.3.3 Flexible structure to enable islanding or closed networks				
1.4 Continue updating GIS database for energy sector	x	x	x	x
Potential Action Items: Tier 1				
1.4.1 Add new energy infrastructure/ assets to database immediately				
1.5 Monitor Automated Critical Asset Management System (ACAMS) for changes	x	x	x	x
1.6 Incorporate DOE Critical Infrastructure Guidelines	x	x	x	x
Potential Action Items: Tier 1				
1.6.1 Identify critical physical assets				
1.6.2 Threat environment				
1.6.3 Policies and procedures				
1.6.4 Physical and cyber security				
1.6.5 Operations security				
1.6.6 Information systems, network infrastructure, and pin testing				
1.6.7 Consequence analysis				
1.6.8 Risk Characterization				
1.6.9 Protection of sensitive information				
1.6.10 Alternative energy sources				

Goal 2: Improve Communication, Coordination, and Public Information

The Potential Initiatives and Potential Action Items included in this table are suggested possible solutions that address many of the capability gaps identified. The Capability Gap Analysis and potential Mitigation Strategy is an identification process only and does not bind any individual agency or utility to the responsibility of implementing any one of the items listed, but encourages continued participation in the EAAG, where energy stakeholders can further investigate processes to approach each item methodically.

Potential Initiative	Preparedness	Response	Recovery / Restoration	Mitigation / Prevention
2.1 Create schedule for maintaining, updating and validating EA plan	x	x		
Potential Action Items: Tier 1				
2.1.2 Create schedule for exercising EA plan				
2.2 Develop restoration working group	x	x	x	
Potential Action Items: Tier 1				
2.2.1 Identify restoration for both utilities and government agencies				
2.3 Governor public service announcement			x	x
Potential Action Items: Tier 1				
2.3.1 Encouraging ration behavior by energy conservation during the "crisis"				
2.4 Create public messaging in advance for energy disruption	x		x	
2.5 Collaborate exercise drill planning and participation	x	x		
Potential Action Items: Tier 1				
2.5.1(a) Conduct exercises				
Potential Action Items: Tier 2				
2.5.1(b) Include Public Health in cross sector exercises				
2.5.2(b) Public/ Private exercises				
2.6 Continue to test Joint Information System	x	x	x	x
Potential Action Items: Tier 1				
2.6.1 State and local messaging via social media				
2.6.2 Coordinating presentations and press releases				
2.6.3 Develop information for targeted audience: legislation, citizen, resident, visitors to state, friends, countrymen, non-English speaking populations				

Goal 3: Expand and Improve Energy Assurance Awareness Through Educational Outreach

The Potential Initiatives and Potential Action Items included in this table are suggested possible solutions that address many of the capability gaps identified. The Capability Gap Analysis and potential Mitigation Strategy is an identification process only and does not bind any individual agency or utility to the responsibility of implementing any one of the items listed, but encourages continued participation in the EAAG, where energy stakeholders can further investigate processes to approach each item methodically.

Potential Initiative	Preparedness	Response	Recovery / Restoration	Mitigation / Prevention
3.1 Develop public awareness campaign	x			
Potential Action Items: Tier 1				
3.1.1 Renew the "keep the lights on" program				
3.1.2 Create check sheets of what the public should do in case of energy disruptions				
3.2 Develop outreach programs	x	x	x	x
Potential Action Items: Tier 1				
3.2.1 Build programs based on targeted audiences				
3.2.2 Utilize press to explain and advertise plans, trainings, exercises in advance				
3.2.3 Trainings				
3.2.4 Webinars				
3.2.5 Conferences				

Goal 4: Pursue Appropriate Reliability and Resiliency

The Potential Initiatives and Potential Action Items included in this table are suggested possible solutions that address many of the capability gaps identified. The Capability Gap Analysis and potential Mitigation Strategy is an identification process only and does not bind any individual agency or utility to the responsibility of implementing any one of the items listed, but encourages continued participation in the EAAG, where energy stakeholders can further investigate processes to approach each item methodically.

Potential Initiative	Preparedness	Response	Recovery / Restoration	Mitigation / Prevention
4.1 Enhance collaboration between utilities and the PUC				x
Potential Action Items: Tier 1				
4.1.1(a) Utilities to conduct cost benefit study of investments to improve resiliency to submit to PUC for consideration of potential cost recovery				
4.1.2(a) PUC to advocate that FERC provide oversight and enforcement of cyber security standards				
4.1.3(a) Pursue shared facility agreements between electric utility providers				
Potential Action Items: Tier 2				
4.1.1(b) Encourage equipment redundancy				
4.1.2(b) Review Nebraska's reliability guidelines (Nebraska Public Power District) for potential legislation model				
4.1.3(b) Increase regional collaboration: Contact Utah, Nebraska				
4.2 Support legislation for enabling rate recovery for redundant transformers and capacitor banks		x	x	
4.3 Explore Mutual Aid Agreements between Utilities for procuring	x	x	x	
4.4 CEO to increase visibility and develop in-house expertise in energy	x			
Potential Action Items: Tier 1				
4.4.1(a) Increase monitoring of energy markets, supply, trends and conditions				
4.4.2(a) Designate preparedness personnel				
4.4.3(a) Monitor regulatory policy				
4.4.4(a) Update Liquid Fuels Plan				
Potential Action Items: Tier 2				
4.4.1(b) Identify Key Process				
♦ Union rules contingency				
♦ Fuels for gasoline consumers				
♦ Emergency contracts				
♦ Fuels Allocation Crisis Plan				

Public Information Strategy

Purpose

The purpose of public information relative to an energy emergency is to establish effective communication capabilities in coordination with the Division of Emergency Management ESF #15 – External Affairs, through the collaboration of ESF #12 co-lead agencies, the Colorado Energy Office and the Public Utilities Commission, should electric power delivery be interrupted or inoperable, in efforts to disseminate accurate information relative to the energy disruption, outage or shortage to the public. This strategy provides a framework for information sharing between ESF #12 and ESF #15.

Scope

An energy emergency of significance which requires State level action will involve many States, local, and private sector agencies collaborating through an organized system to provide educational strategies and disseminate information accurately and efficiently that will contribute to public safety and welfare throughout the event.

The Joint Information System (JIS) as established under the National Incident Management System (NIMS) will be used for the purposes of the Plan. It provides the mechanism for personnel with public information responsibilities from all affected jurisdictions or entities to organize, integrate, and coordinate information to ensure accuracy, rapid accessibility, and consistency in messaging of critical information. A JIS has three components; the Public Information Officer (PIO) or personnel with public information responsibilities, the methods used to provide public information, and the Joint Information Centers (JICs), which are locations where such personnel perform public information functions. A single location is preferable though many may exist until multi-jurisdictional incident management is established.

Situation and Assumptions

- The public needs timely and accurate information for protection of life, the environment, and property
- Local jurisdictions will provide immediate and vital information to local public
- Regulated private utilities report outages to the PUC
- Private utilities inform affected customers
- Unregulated utilities report outages through WECCnet
- Liquid Fuels shortages are monitored by CEO
- CEO and PUC through ESF #12 collect and report outage information to DEM
- DEM will provide accurate and timely information to the Governor
- DEM PIO utilizes the JIS to disseminate information to the public
- The Emergency Alert System may be used for public alerts – ESF #2 Communications

Concept of Operations

- Utilize the National Incident Management System (NIMS) for Public Information component
- The Division of Emergency Management (DEM) PIO will be the central point of contact for establishing the JIS.
- A JIC may be established by DEM PIO
- ESF #12 co-lead agencies will collaborate with their respective PIO and establish liaison between ESF #12 and the JIS.
- Media relations, news briefings and press conferences are established through the JIS.

Roles and Responsibilities

Division of Emergency Management Public Information Officer During an Event
<ul style="list-style-type: none"> ✓ Central Point of Contact (POC) for establishing the Joint Information System (JIS) ✓ Initial establishment of the Joint Information Center (JIC) ✓ Responsible for scheduling news briefings for key disaster officials, writing and disseminating news releases to appropriate media outlets, monitoring and analyzing TV, radio, and newspaper disaster news coverage and providing this information to the JIS. ✓ Responsible for preparing background information and fact sheets.

Colorado Energy Office Public Information Responsibilities During Normal Operations
<ul style="list-style-type: none"> ✓ Media relations and monitoring on energy issues ✓ CEO website preparation and design ✓ Materials preparation of energy related presentations/speaking for both the governor and the CEO director ✓ Press releases ✓ Increase energy information and understanding in Colorado

**Public Utilities Commission
Public Information Responsibilities
*During Normal Operations***

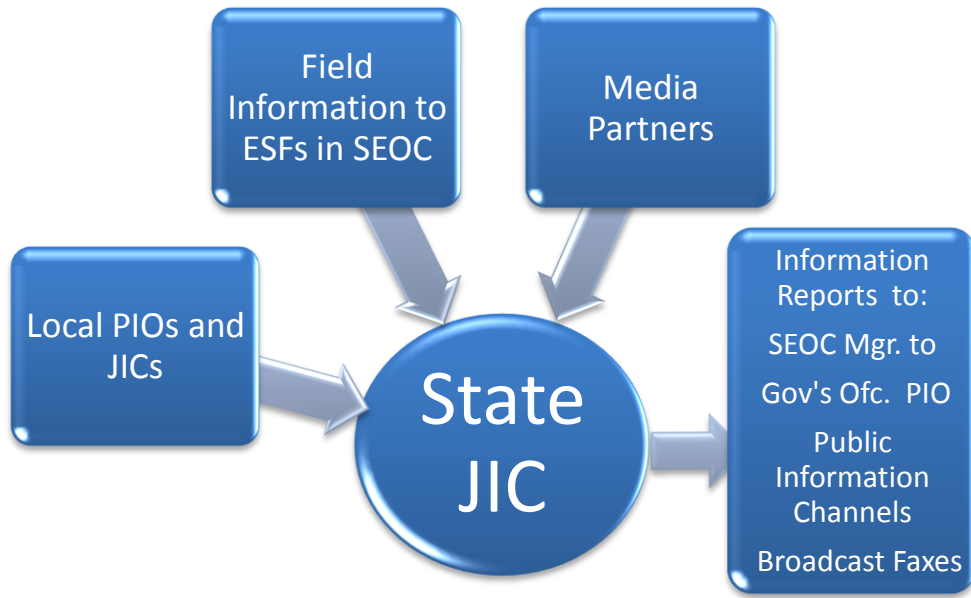
- ✓ PUC PIO coordinates communication for the general public on Public Utilities Commission activities such as utility regulation and rate cases that pertain to electric energy, transportation, natural gas, steam and others.
- ✓ The PIO also maintains the Commissions website with newsletters, and public hearing announcements such as the weekly Commissioner Meeting held every Wednesday of each week.
- ✓ In addition, the Information Officer manages internal communications to be shared within the various groups of the Division as well as with the Department of Regulatory Agencies and other State agencies.
- ✓ The PUC PIO responds to inquiries from the general public when major utility outages occur and when the PUC is providing support to the State’s Emergency Operation Center when major energy related impacts occur.
- ✓ The PIO also manages a comprehensive public information program that insures the public is aware of rulemaking processes so that the opportunity for input by the public is provided.
- ✓ The PUC PIO also manages the “Consumer Assistance Group” that deals with complaints from customers of utility companies and assists in finding resolutions to these service complaints.

**Colorado Energy Office & Public Utilities Commission
Coordination of Public Information
During an Event**

- ✓ Collect information from subject matter experts related to the event
- ✓ CEO’s website can be a tool to help with messaging during an event
- ✓ CEO and PUC collaborate with respective PIOs to integrate information and disseminate public messaging through the Division of Emergency Management PIO (ESF #15)
- ✓ Maintain communication with utilities for outage updates and restoration schedule

In Figure VIII-9, an organizational chart depicts how the Joint Information System works.

Figure VIII-9 Joint Information System (JIS)



Book 3

Part 1 Energy Sector Risk and Vulnerability Assessment

The Risk and Vulnerability Assessment educates the reader about Colorado’s energy blueprint with a focus on the threats, risks and vulnerabilities to the overall energy sector, and the crucial importance of reliability on the electric sector from all other sectors of society.

Book 3 Table of Contents

IX. Risk and Vulnerability Assessment	1
Assessing Existing Publications, Planning Mechanisms, Reports, and Studies	1
<i>Introduction</i>	1
<i>Renewable Energy Publications</i>	1
<i>Climate Related Initiatives</i>	7
<i>State and Regional Plans, Reports, and Studies</i>	8
<i>Risk Related Standards, Reports and Studies</i>	9
<i>Alignment with National and State Planning Mechanisms</i>	10
<i>State Framework for Emergency Management</i>	12
<i>Establishing the EA Communications Framework</i>	15
<i>Local Energy Assurance Plans</i>	18
Energy Sector Profile	20
<i>US and Colorado Electric Power Systems</i>	20
<i>Colorado Grid System Risks</i>	31
<i>Trends in the Industry</i>	32
Colorado Energy Resource Profiles.....	35
<i>Natural Gas</i>	35
<i>Renewable Resources</i>	44
<i>Coal</i>	55
<i>Hydroelectric</i>	60
<i>Liquid Fuels</i>	63
Smart Grid and Distributed Generation	70
<i>Smart Grid Considerations in the Colorado Energy Assurance Emergency Plan (CEAEP)</i> ...	70
<i>Distributed Generation Considerations in the Colorado Energy Assurance Emergency Plan</i>	72
<i>Smart Grid and Distributed Generation Vulnerabilities</i>	74
Colorado Energy Sector Asset Database	77

Costs and Strategic Approaches to Disruption	80
<i>Understanding the Costs of Energy Disruption</i>	80
Energy Sector Interdependencies.....	85
<i>Interdependencies and Systemic Failures</i>	88
<i>Energy Infrastructure Interdependency Failures: Case Studies</i>	90
High Impact Low Probability (HILP) Events.....	97
<i>Cyberwarfare</i>	97
<i>Solar Weather</i>	112
Exercises	131
<i>Introduction</i>	131
<i>Organization</i>	131
<i>Intra/Inter-State Exercise: Cyber Attack</i>	132
<i>Inter-State Exercise: Geo Magnetic Storm</i>	143
<i>Western Region Energy Assurance Exercise</i>	151

The CEAEP is a comprehensive document that includes background information, reference materials, and other subject matter that may not be of interest to all readers. As a convenience, suggested sections are identified below for specific audiences.

For State Agencies and Local Emergency Management Stakeholders

- Risk and Vulnerability Assessment
 - Interdependencies
 - HILP Events
 - Exercises

For Energy Stakeholders

- Risk and Vulnerability Assessment
 - Interdependencies
 - HILP Events
 - Exercises

For Utilities

- Risk and Vulnerability Assessment

IX. Risk and Vulnerability Assessment

Assessing Existing Publications, Planning Mechanisms, Reports, and Studies

Introduction

An initial risk and vulnerability assessment should include assessing existing subject-related documents intended to provide guidance, establish a plan of action, change law, policy, regulations or codes, and/or provide critical data in evaluating whether a proposed action is viable or not. This subsection is an introductory and cursory attempt to analyze and understand the role that existing planning mechanisms play as an element of a jurisdiction's capability or lack of capability. A community or jurisdiction's capability, in this case the State of Colorado, to respond and recover from an impactful incident is directly related to its governing body and the existing laws, policy, regulations, standards, and codes supported by the actual research and data that led to the development of such planning mechanisms. The following is a selected list of activities and related documents that have been assessed in the EA Planning process to establish a level of capability for responding to and recovering from an energy emergency as well as building energy assurance. This assessment establishes the alignment of State to Federal, State to State, State to local, and State to private sector response and recovery capability.

In the Community Profile section, some legislative activities were highlighted in relationship to renewable energy solutions and the role of the CEO in the management of energy sector issues. Some publications related to those legislative activities are summarized here. Although the main focus of the selected planning mechanisms is to substantiate Colorado's progress in building energy assurance, they also link CEO's activities to other State agencies' activities that collectively build overall in-house and regional capability to respond and recover from an energy sector disruption.

The succeeding subsections will focus on Colorado and the U.S. energy sector specifics, to include current Colorado energy statistics, emphasizing interdependencies and the cost and causes of energy disruption. The final subsection is a value-added element in the Risk and Vulnerability Assessment section, which is an in-depth energy sector hazard typology and risk probability assessment.

Renewable Energy Publications

Connecting Colorado's Renewable Resources to the Markets – SB 07-091 Report, Dec. 21, 2007

Colorado Senate Bill 07-091, Report of the Task Force for Renewable Resource Generation Development Areas: The Task Force was given the charge to map the renewable resources throughout the State of Colorado. This report contains maps of these resources and identifies

“Generation Development Areas” where the resource can be developed with competition among developers for utility-scale wind and solar projects. The report also identifies local development opportunities for geothermal, hydroelectric power, biomass, and ethanol. The maps identify existing generation and where high voltage transmission is needed to bring renewable resources to the markets.

Link to Report:

- http://www.energy.ca.gov/reti/documents/2007-12-21_CO_%20SB91_Task_Force_Report.pdf

Connecting Colorado’s Renewable Resources to the Markets in a Carbon-Constrained Electricity Sector -Renewable Energy Development Infrastructure: REDI Report Dec. 2009

This publication ensures Colorado’s ability to move forward with an energy assurance strategy. It serves as a comprehensive analysis of the potential for renewable energy development in Colorado and its recommendations for ground-breaking progress to meet the goals of SB 07-91, reducing carbon dioxide emissions by 20% by the year 2020. It is essentially a CO₂ reduction plan. In efforts to do so, the REDI report identifies generation development areas and the challenges of bringing renewable power to the demand markets. Initial steps would include the need to greatly increase investment; accelerate construction; increase the use of natural gas while reducing the number of coal operated plants; the development of a long range transmission plan where a balancing authority would pay special attention to Colorado’s wildlife, lands, scenic and natural resources. Colorado would need robust participation incentives. To develop a strategy, consumption trends were first analyzed. Three modeling scenarios were conducted to project where Colorado would be if:

- 1) The current energy demand and consumption rate were to continue;
- 2) The expected “reduced” demand and consumption were maintained; and,
- 3) A scenario which writes the formula to arrive at the answer by working in reverse. What will it take to actually accomplish those 2020 goals?

Each scenario pointed to the level of dedication needed to accomplish success. Changes in regulatory and policy structure to reflect new programs would be necessary; Implementing an aggressive demand-side measures strategy and enforcing it would be challenging but critical; Planning for a carbon constrained environment was dependent upon buy-in and compliance from providers as well as consumers; The “how-to’s” for balancing power generation and demand; Monitoring flows for heating limits; Systems planning, design and maintenance; Demand-response by changing the timing using automated controls - Smart Grid technologies; and benefactors of distributed generation are but a few examples of an aspiring successful renewable energy portfolio. Through each phase of implementation consideration to local, state, and federal affairs, private enterprise, energy conservation, efficiency, infrastructure, population growth and much more would have to be the operating picture. A Transmission Task Force on Reliable Electricity Infrastructure was established for oversight.

Link to Report:

- <http://www.colorado.gov/cs/Satellite?blobcol=urldata&blobheadername1=Content-Disposition&blobheadername2=Content-Type&blobheadervalue1=inline%3B+filename%3D%22REDI+Report+%28Full+Version%29.pdf%22&blobheadervalue2=application%2Fpdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1251746588129&ssbinary=true>

Colorado's Generation and Transmission Baseline Study – 2009

This study is a portion of the REDI that looks at CO's generation and transmission infrastructure by examining the existing power system, and the factors involved in achieving maximum economic societal benefits from electricity production from conventional and renewable resources.

- **Generation:** A successful large-scale shift to clean energy which demands a bold commitment by utilities, regulators, and policymakers for power to be delivered to consumers efficiently and economically.
- **Transmission:** The transmission system in Colorado is stressed and is in urgent need of improvement investment. Improving transmission capacity is a key to expanding future development of wind and other variable renewable resources in Colorado.
- **Senate Bill 07-100:** The new law affects Colorado utilities that are subject to rate regulation by the Colorado Public Utilities Commission (PUC). It directs the PUC to allow current recovery of the costs of planning, developing and completing the construction or expansion of transmission facilities that have been approved by the PUC through a separate rate adjustment clause that can be changed annually. Also allows PUC to grant certificates of public convenience and necessity (CPCN) for new transmission facilities serving GDAs needed by utilities in order to comply with the Renewable Energy Standard (RES) Amendment 37, HB 10-1001.
- **Larger Balancing Authority**

Link to Report:

- <http://cospl.coalition.org/fez/eserv/co:8449/gov112g282009internet.pdf>

A Blueprint for a New Energy Economy

This publication tells the story of Colorado's New Energy Economy, as established by former Governor, Bill Ritter, Jr. Key elements ensure long-term market transformation, which has taken into consideration jobs, protection of the state's beauty and its clean, inexhaustible energy. Uniting researchers and the private sector through the Colorado Renewable Energy Collaboratory to train the next generation of scientists and engineers would reinforce the reputation of Colorado as a leader in renewable energy. The National Renewable Energy Laboratory (NREL) would partner with Colorado's three major research universities: the

University of Colorado, Colorado State University and the Colorado School of Mines. NREL is the only federal laboratory dedicated to the research, development, commercialization and deployment of renewable energy and energy efficient technologies. It is “focused on advancing the U.S. Department of Energy’s and the nation’s energy goals with areas of expertise including renewable electricity, renewable fuels, integrated energy system engineering and testing, and strategic energy analysis.” (Source: Blueprint for a New Energy Economy)

Link to Report:

- <http://www.colorado.gov/cs/Satellite/GovEnergyOffice/CBON/1251597774824>

2010 Utilities Report

This report is Colorado’s Electric and Gas Industries publication, which provides a profile on 65 electric and gas utilities. Current statistics are provided in subsequent subsections.

Link to Report:

- <http://www.colorado.gov/cs/Satellite?blobcol=urldata&blobheadname1=Content-Disposition&blobheadname2=Content-Type&blobheadvalue1=inline%3B+filename%3D%222010+Utility+Report.pdf%22&blobheadvalue2=application%2Fpdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1251760307078&ssbinary=true>

Deploying Smart Grid in Colorado - Colorado Smart Grid Task Force, Created by SB 10-180

This publication is the result of a study on the feasibility, cost, and timing of transitioning to a secure, resilient, and technologically advanced electric grid known as the “Smart Grid.” Its focus included:

- Challenges and Opportunities in Colorado
- Workforce and Economic Development,
- Consumer Issues and Data Management,
- Distributed Energy Resources and Grid Management
- Technical Specifications
- Grid Operations

Results suggested:

- Colorado positioned for Smart Grid implementation
- Requires coordination and commitments from universities, research laboratories, and electricity industry for economic development opportunities
- Consumer education and outreach needed

- Smart Grid will make greater use of distributed energy resources, which reduce emissions and utilize electricity from renewable resources
- Technical standards and specifications need to be developed and implemented
- Increased monitoring, automation, and load-shifting ability, and increased solar participation from customers is essential to maintain reliability
- Smart Grid should be implemented at a gradient depending upon how quickly the transition is expected to take place.
- Winter weather (including heavy snow and ice) is the most frequent and costly natural hazards to damage utility CI. It was also rated by the most REC's as High or Medium impact by hazards.
 - Next two (tied) were Fire and Lightning, with Windstorms close behind.
- Distribution Lines and Transformers were rated as most critical CI to electric infrastructure system, with transmission lines and control center close behind

Link to Report:

- <http://www.colorado.gov/cs/Satellite?blobcol=urldata&blobheadername1=Content-Disposition&blobheadername2=Content-Type&blobheadervalue1=inline%3B+filename%3D%22Smart+Grid.pdf%22&blobheadervalue2=application%2Fpdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1251769834847&ssbinary=true>

Solar PV and Small Hydro Valuation – R.W. Beck/SAIC – 2011

This study was an element of the EA Initiative to consider Smart Grid and Distributed Generation technologies. It included:

- Conduct a quantitative analysis of the hourly demand, loads, and the current projected renewable resources for the utility partners as a foundation for determining the individual production characteristics for solar PV and hydro.
- Determine the value of distributed generation resources by accumulating the sum of individual benefits from energy, avoided capacity, emission reductions, loss savings, grid resiliency, and disaster recovery savings.
- Identify the related cost and other impacts from distributed renewable resources and balance them against the identified benefits to assist the utility partners in building their own business case(s) for continued implementation of distributed renewable energy resource programs.
- Review each utility's specific results in a broader and integrated context to identify common issues and results that support the CEO in its mission of promoting state-wide energy policies

The study suggests:

- High potential for real monetary value to smaller utilities.

- Majority of utilities can derive benefit – near or long term– in supporting, and in some cases incenting, renewable generation in both small hydro and solar PV.
- Solar PV, hydro and other renewable energy systems, even at utility scale, are not a replacement for conventional generation, but rather a sound component of a balanced generating portfolio to serve Colorado.

Distributed Generation Benefits:

- Solar PV could improve customer reliability if industry standards allowed “islanding” so that solar PV could provide power during a local or system outage. Existing standards do not allow this practice because generation into the power grid without utility knowledge or control poses a safety hazard to utility personnel. This practice would also require sophisticated metering and control systems to match the load with the solar PV at any given instance. AMI and Smart Grid technology could provide the communications link to address these concerns and lead to changes in these restrictions. (See Section 3 of this Report for discussion of Grid Resiliency and distributed solar PV systems.)

Thirty-Five Percent Wind and Solar Integration Study

This Study was “to investigate operational impact of up to 35% energy penetration of wind, PVs, and concentrating solar power on the power system operated by the WestConnect group of utilities in AZ, CO, NV, NM, and WY.

- Technical analysis indicates that it is feasible for the WestConnect region to reach 30% wind and 5% solar energy penetration, provided there are key changes to current practice.
 - Balancing area cooperation
 - Sub-hourly scheduling (because of variability)
 - Access to underutilized transmission capacity
- Variability of renewable energy impacts its utility
- Challenges and potential of large-scale integration of wind and solar include
 - Characterization of the capabilities of the non-renewable generation portfolio in greater detail (e.g., minimum turndown, ramp rates, cost of additional wear and tear)
 - Changes in non-renewable generation portfolio (e.g., impact of retirements, characteristics, and value of possible fleet additions or upgrades)
 - Reserve requirements and strategies (e.g., off-line reserves, reserves from non generation resources)
 - Fuel sensitivities (e.g., price, carbon taxes, gas contracts and storage, hydro constraints and strategies)
 - Load participation or demand response (e.g., functionality, market structures, PHEV)
 - Forecasting (e.g., calibration of forecasting using field experience, strategies for use of short-term forecasting)
 - Rolling unit commitment

- Transmission planning and reliability analyses
- Hydro flexibility

Link to Report:

- <http://www.nrel.gov/docs/fy10osti/47781.pdf>

Climate Related Initiatives

The Plan is designed to understand and be prepared for all risks that may pose a threat to Colorado’s energy infrastructure. The potential challenges from anthropogenic climate change are important because they represent a real risk necessitating management.

Colorado Climate Action Plan 2007

November 2007, the Colorado Climate Action Plan was published laying out a path to reduce greenhouse gas emissions 20 percent by 2020 by

- Provide Greener Electricity
- Research and Innovation for Coal, Natural Gas and Renewable Energy
- Recycle/Solid Waste
- Report Emissions
- Lead by Example
- Regional Carbon Emissions Trading
- Foster an Educated Workforce
- Adapt to Climate Change

Link to Report:

- <http://www.pewclimate.org/docUploads/COClimatePlan.pdf>

Intergovernmental Panel on Climate Change Reports

The IPCC is a scientific body. It reviews and assesses the most recent scientific, technical and socio-economic information produced worldwide relevant to the understanding of climate change. It is comprised of three working groups.

- The IPCC Working Group I (WG I) assesses the physical scientific aspects of the climate system and climate change
- The IPCC Working Group II (WG II) assesses the vulnerability of socio-economic and natural systems to climate change, negative and positive consequences of climate change, and options for adapting to it. It also takes into consideration the inter-relationship between vulnerability, adaptation and sustainable development.

- The IPCC Working Group III (WG III) assesses options for mitigating climate change through limiting or preventing greenhouse gas emissions and enhancing activities that remove them from the atmosphere. The sectors include energy, transport, buildings, industry, agriculture, forestry, waste management.

Climate Change – Regulatory Initiatives

- Large emitters of greenhouse gases (GHG) are required by the U.S. Environmental Protection Agency (EPA) to begin collecting GHG emissions data under a national reporting system, beginning as early as January 1, 2010. The reporting covers approximately 85 percent of the nation’s GHG emissions and 10,000 facilities. This reporting rule is called the Mandatory Reporting of Greenhouse Gases Rule, promulgated in October 2009.
- Additionally, large stationary sources of GHG are required under the Prevention of Significant Deterioration (PSD) and Title V Operating Permit programs to obtain permits for construction or operation of their facilities effective January 2, 2011. The EPA has estimated that this will affect an additional 550 facilities nationwide, up to 15,550 in total. This permitting related rule is called the Prevention of Significant Deterioration and Title V Greenhouse Gas Tailoring Rule, promulgated in June 2010, and commonly called the Tailoring Rule.

State and Regional Plans, Reports, and Studies

2007 State Energy Emergency Response Plan (SEERP)

The predecessor to the Colorado Energy Assurance Emergency Plan was reviewed in full to evaluate any existing gaps in the Plan and utilize pertinent data appropriately.

2009 Liquid Fuels Plan – Revised 2012

Colorado’s Liquid Fuels Emergency Action Plan, which is an emergency crisis action guide in the case of a liquid fuels shortage or disruption.

State Natural Hazards Mitigation Plan (2010)

This Plan is crucial to State assets and associated natural hazard zones. A risk and vulnerability assessment is conducted every three years to update this plan by strict FEMA Hazard Mitigation Regulations. Areas and assets most vulnerable to specific hazards and hazard zones are cited and mapped by county. A mitigation strategy is then developed to address those most at risk.

Link to Plan:

- www.colorado.gov/cs/Satellite/DOLA-MAIN/CBON/1251595686517

Colorado Rural Electric Natural Hazards Mitigation Plan – 2010

This plan is a natural hazards mitigation plan for rural electric providers as part of the State Natural Hazard Mitigation Plan that meets or exceeds federal standards while strengthening disaster resilience and recovery capabilities of the State’s rural electric providers.

- Hazards include blizzards, ice storms, windstorms, tornadoes, fires, landslides and floods

Link to Plan:

- <http://www.colorado.gov/cs/Satellite?blobcol=urldata&blobheadername1=Content-Disposition&blobheadername2=Content-Type&blobheadervalue1=inline%3B+filename%3D%22Colorado+Rural+Electric+Natural+Hazards+Mitigation+Plan.pdf%22&blobheadervalue2=application%2Fpdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1251770660702&ssbinary=true>

Drought Hazard Response and Mitigation Plan

A comprehensive risk and vulnerability assessment on the Drought hazard, which is also an annex to the State Natural Hazard Mitigation Plan, developing a response strategy and mitigation actions to reduce the impacts of Drought. An element of the Plan examines the impacts on the Energy Sector.

Tri-State Crisis Management Procedures

This document is a crisis procedure manual for energy emergencies that impact Tri-State Generation and Transmission assets and services.

Risk Related Standards, Reports and Studies

Cyber Security Standards - NIST IR 7628

This publication of standards is delivered by the Smart Grid Interoperability Panel-Cyber Security Working Group of the National Institute of Standards and Technology Interagency Reports. It is a comprehensive security analysis of the Smart Grid from the bottom up to include logical architecture and interfaces. It offers a set of guidelines that should be considered, at a minimum, for securing a Smart Grid environment from cyber attack.

Link to Report:

- http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf

Roadmap to Achieve Energy Delivery Systems Cyber Security - 2011

This report outlines a strategic framework over the next decade among industry, vendors, academia, and government stakeholders to design, install, operate, and maintain a resilient energy delivery system capable of surviving a cyber incident while sustaining critical functions.

Link to Report:

- http://www.cyber.st.dhs.gov/wp-content/uploads/2011/09/Energy_Roadmap.pdf

Geomagnetic Storms and Their Impact on the U.S. Power Grid – Metatech, 2010

A comprehensive analysis of the impacts of a Geomagnetic Storm on the Electric Grid.

Link to Report:

- http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf

Global Risk – 2012: an Initiative of the Risk Response Network

A global Risk Response Network Initiative. This Initiative is a comprehensive global analysis of the vulnerabilities and risks from a global perspective. In short, the failure of government systems and cyber security are among the highest risks with the most uncertain response solution.

Link to Report:

- <http://www.weforum.org/reports/global-risks-2012-seventh-edition>

Alignment with National and State Planning Mechanisms*The National Framework for Disaster Management*

Integrating an Energy Assurance Plan into existing National and State planning mechanisms is complex in that “traditional” energy plans normally outline actions to be taken in the effort to accomplish an energy conservation goal, efficiency goal, emissions reduction, or a goal to implement renewable energy facilities, where an Energy Assurance Plan must incorporate the philosophy of comprehensive emergency management best practices into the framework of a traditional Energy Plan. It is not a perfect fit. Enhancing energy reliability from the perspective of emergency preparedness and response, or recovery and mitigation programs can be extremely difficult. The energy industry with its complicated power delivery systems and its interdependencies on sector-specific operations doesn’t allow for a simplified process to identify implementable actions during an emergency that will assist utilities in power delivery continuity; however blending strategies that includes focusing on potential risk and vulnerabilities while

building a new energy portfolio will help those that monitor such systems to recognize early symptoms of a potential energy disruption. Strategies that create solid partnerships between the utility professional and the emergency management practitioner can provide a workable framework to accomplish goals from both perspectives.

The National Response Framework (NRF)

The NRF defines the; **who, what, and how** of core response concepts that can be applied at all levels of government. It stresses the **importance of planning** and the necessity for a **resource support network** with the intention for State and local governments to adopt and apply it. The NRF is a response policy and an operational coordination doctrine intended to accelerate incident assessment and response. It promotes unity and influences the manner in which policy and plans are developed. The five key principles are to (1) engaged partnership, (2) tiered response, (3) scalable, flexible, and adaptable operational capabilities, (4) unity of effort through unified command, and (5) readiness to act. The National Incident Management System (NIMS) and the Incident Command System (ICS) are management and operational systems that provide a structure for multiple agencies to coordinate effectively in an Emergency Operations Center (EOC) and on scene of an incident. The Emergency Management Assistance Compact (EMAC), is a congressionally ratified compact, which is a mechanism by which one state can ask for resource assistance from any other state that is an EMAC participant. An essential element of these structure templates is the necessity to clarify the roles and responsibilities of all levels of players in disaster operations, which includes: Local Governments; State, Territories, and Tribal Governments; Federal Governments; and the Private Sector and Non-Governmental Organizations. Engaging all partners in activities that enhance preparedness greatly increases the strength of united capabilities. In building a comprehensive emergency management program establishes a proactive attitude rather than a reactive attitude.

The development of the Plan is based upon the principles of the NRF and the **National Homeland Security Strategy**, which is supported through other strategies, plans and ongoing efforts. It further compliments the National Infrastructure Protection Plan (NIPP) by serving as a tool to address response and recovery activities specific to the energy sector's critical infrastructure and key resources (CIKR). National Priorities and Scenarios were taken into consideration in the design of the Intra-State and Inter-State Exercises facilitated for Colorado's energy sector and emergency management stakeholders. Lessons learned were incorporated into the Plan, which provides four strategies detailed in the Action Plan Section, which addresses Response, Recovery, Mitigation, and Public Information.

NRF Website: <http://www.fema.gov/emergency/nrf/>

U.S. Department of Energy Strategic Plan

This Plan focuses on America's security and prosperity by addressing its energy, environmental, and nuclear challenges and seeks to create economic competitiveness through science and technology. It intends to answer the need to minimize nuclear threats while simultaneously

building a new nuclear framework. It is a strategy to deploy existing technologies and accelerating new technologies to advance national conversation on energy. It includes a strategy for additional research in subatomic physics, climate science, chemicals and materials. This agency hopes to increase transparency to strengthen the energy sector as a whole by partnering with the private sector, and supporting the scientific community and its findings.

DOE Strategic Plan Website: http://energy.gov/sites/prod/files/2011_DOE_Strategic_Plan_.pdf

Blueprint for a Secure Energy Future - The White House, 2011

A Blueprint for securing America’s Energy Supplies by expanding safe and responsible domestic oil and gas development and production and by leading the world toward safer, cleaner and secure energy supplies. It provides:

- Consumers with choices to reduce costs and save energy by reducing costs at the pump with more efficient cars and trucks and cutting energy bills with more efficient homes and buildings.
- A process to a clean energy future by harnessing America’s clean energy potential, clean energy research development, and leading by example with the federal government.

Link to the Report:

- http://www.whitehouse.gov/sites/default/files/blueprint_secure_energy_future.pdf

Energy Security in the United States – Congressional Budget Office, May 2012

This report provides a snapshot of the vulnerability of Energy Markets and potential impacts of disruptions. It displays energy consumption statistics and comparisons charts, addresses the global market oil production capacity, electricity generation spare capacity and flexibility, transportation sector impacts, options for reducing energy costs, and promoting policy change to reduce the impact on the consumer.

Link to the Report:

- <http://www.cbo.gov/sites/default/files/cbofiles/attachments/05-09-EnergySecurity.pdf>

State Framework for Emergency Management

Division of Emergency Management (DEM)

The Division of Emergency Management was organized to establish the State’s Emergency Management Program. It functions under the Department of Local Affairs working alongside other State agencies that have a role in local government responsibilities. DEM’s role in the development of the CEAEP involves collaboration between the various State agencies and non-governmental organizations that not only have a stake in local government, but also in the energy

sector. DEM has long since established a State agency network of emergency response coordinators. DEM's collective knowledge and vast experience in State emergency and disaster operations has provided a special component to the development of the CEAEP. Once initial planning efforts were established, DEM's role took on more responsibility in the development of a collaborative response, recovery and mitigation strategies. DEM has established relationships with the players at every level of government. Their role is advisory and often offers technical assistance regarding the interpretation of the Code of Federal Regulations (CFR) pertaining to the disaster declaration process and how public and/or individual assistance after a disaster is determined and allocated. DEM also has a long history of Federal funding grantsmanship. They are the conduit for streamlining funds from the Federal Emergency Management Agency to local communities for much needed hazard mitigation projects as well as providing State funding for the Flood Mitigation Assistance program, to mention a few. DEM is responsible for the implementation of the State Emergency Operations Plan.

State Emergency Operations Plan (SEOP)

The SEOP consists of a base document that identifies the state structure for managing emergencies and the activities necessary to support response efforts to a local emergency or disaster, and supporting annexes further defining emergency support sectors and their functions. During a disaster DEM activates or “stands up” the State Emergency Operations Center (SEOC). If the disaster situation warrants, DEM will request representatives from other State agencies and affiliated organizations that have the authority to procure resources in support of the disaster operations, to respond to the SEOC. This activated network of State agencies and other affiliated organizations work together throughout the disaster to support the resource needs to manage the event until a state of normalcy can be regained. The SEOP aligns its plan structure with that of the National Response Framework adopting the Emergency Support Function (ESF) format. It identifies the roles and responsibilities of this network by clarifying the function in terms of 15 different emergency support functions of society and who or what agency is responsible to provide the resources affiliated with that function. ESF #12 is the ESF that defines the “energy” sector and which State agencies have been identified, and have mutually agreed to act as the Co-Lead Agencies that will coordinate information and/or resources in support of disaster operations. Each lead agency representing an ESF is encouraged to develop their own emergency response and recovery strategy similar to the Sector-Specific Plans found in the National Infrastructure Protection Plan (NIPP). The development of the CEAEP serves as a component of the Energy Sector-Specific Plan for Colorado. It is a tool in coordinating response, recovery and mitigation activities relative to the electric grid, electric power delivery systems, and their interdependencies during electric power disruption or outage events. The Liquid Fuels Emergency Action Plan, completed in 2009, serves as a crisis action guide during incidents involving shortages of petroleum fuels.

Link to the SEOP:

- <http://www.colorado.gov/cs/Satellite?c=Page&childpagename=DOLA-Main%2FCBONLayout&cid=1251595696267&pagename=CBONWrapper>

ESF #12 – Energy

The term “energy” includes production, refining, transporting, generating, transmitting, and distribution components. The purpose of ESF #12 is “to coordinate the restoration and protection of Colorado’s critical electricity generation, transmission and distribution infrastructure, and the supply of fuels used in base load generation (natural gas and coal) following a major disaster, emergency, or other significant event” (SEOP). DOE, the Federal ESF #12 Lead Agency in the NRF, envisions “a robust, resilient energy infrastructure in which continuity of business and services are maintained through secure and reliable information sharing, effective risk management programs, coordinated response capabilities, and trusted relationships between public and private partners at all levels of industry and government.”

An Emergency Action Plan for Liquid Fuels was created in 2009 and is currently undergoing revision. This Plan is a companion document to the Liquid Fuels Emergency Action Plan. Together they provide general response guidance and recommendation for improved energy emergency operations.

Supporting argument for CEO to represent ESF #12 as a Co-Lead team:

- The Public Utilities Commission (PUC) was originally identified as the Lead Agency for ESF #12 based on misinformation that the PUC had established and maintained contracts with the utilities companies and therefore could coordinate resources in conjunction with the utilities in the event of an energy disruption. This of course is not the case given the role and responsibilities of the PUC as a regulatory agency. Their role is specifically, among other things to enforce State mandated regulations and address rate case requests by the regulated utilities companies.
- Regulated Utilities are accountable to the PUC; however non-regulated utilities are affiliated with CEO. Depending on what energy sector is impacted by an energy emergency, one or both agencies may need to act as the ESF #12 representatives to DEM.
- The PUC and CEO are identified co-leads for ESF #12 functions; however, CEO is the agency specifically responsible for liquid fuels in the Liquid Fuels Emergency Action Plan. The Colorado Energy Office plays a key role in coordinating with liquid fuels energy sector and other agencies during a fuels shortage situation. Other agencies include: The Department of Public Health and Environment (CDPHE) (pollution control standards) responsible for the regulatory oversight for liquid fuels contamination to the environment; The Department of Labor and Employment (CDLE) (storage, weights and measures) responsible for the standards for fuels storage; The Colorado Department of Public Safety is responsible for the transportation of liquid fuels; and, the Division of Natural Resources - Oil and Gas Conservation Commission, who has authority over the production of oil and gas. The PUC and CEO are the appropriate Co-Leads for ESF #12.

- Department Heads from all three State agencies agreed that CEO should share a Co-Lead with the PUC in the SEOC.

An ESF Lead Agency representative is required to participate in preparedness activities, as stated in the State Homeland Security Strategy. DEM has established requirements for representatives of ESF Lead Agencies, which are referred to as a State-agency Emergency Response Coordinator (ERC).

Requirements include:

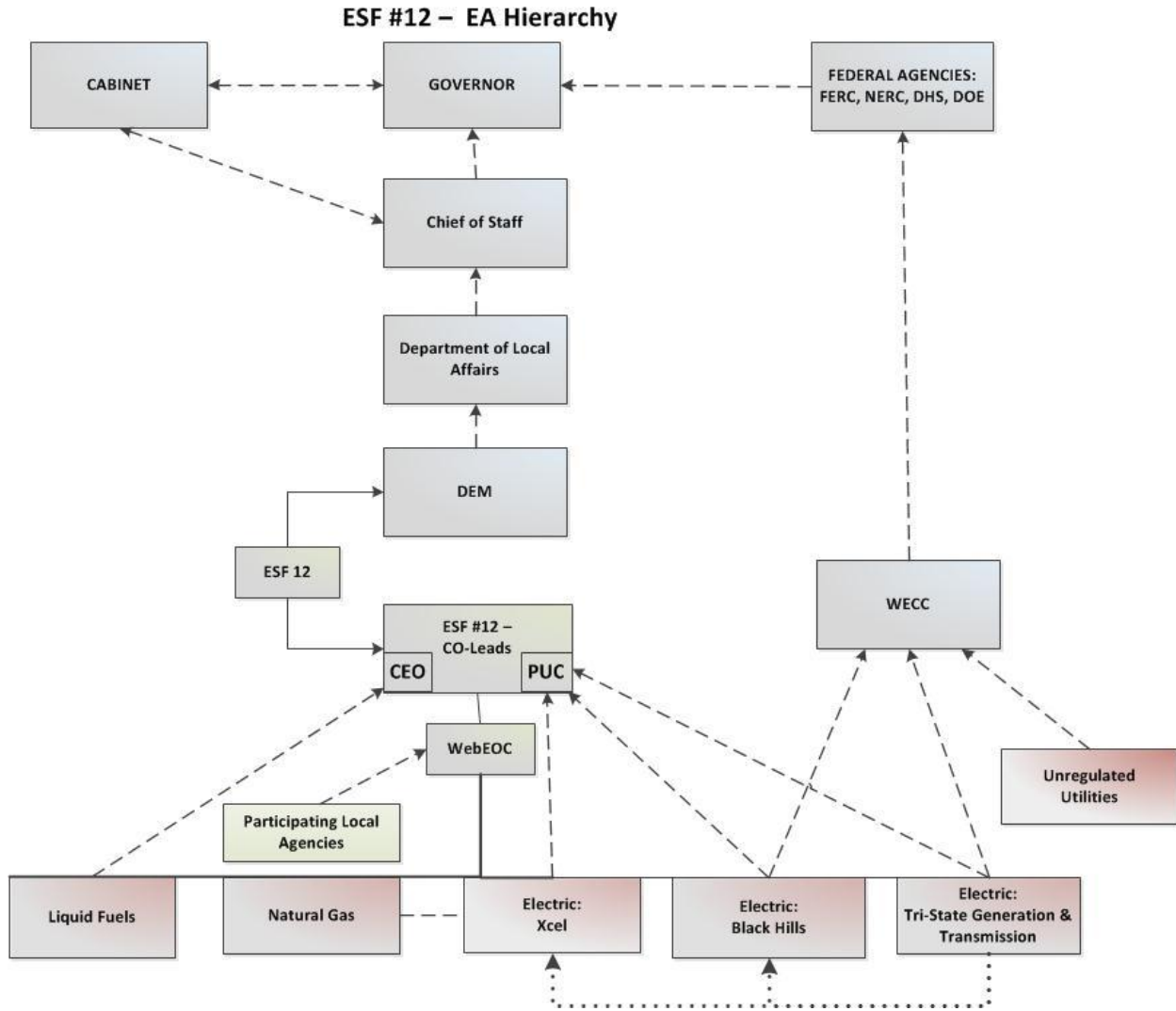
- If applicable, the ERC *is* the lead agency representative for a specific ESF as outlined in the SEOP.
- ERC will provide support through staff, technical services, and/or equipment to other ESF Lead Agencies.
- Occupy a seat at the SEOC during the Center’s activation, at the direction of the Director, Division of Emergency Management.
- Participate in SEOC exercises and associated training sessions, which may include WebEOC®, SEOC management and forms usage, NIMS training such as, Position Specific Command and General Staff training, etc.
- During periods of non-activation of the SEOC, be aware of on-going incidents and relay applicable information to DEM (for example: electric transmission lines, transformers, natural gas pipeline, etc. damage or the correction of false reports in reference to infrastructure damage)
- Assist in the periodic review and update of the SEOP due to lessons learned and/or new Federal guidance. (Updates to the SEOP are conducted after an actual event in Colorado or elsewhere that would improve response or after exercises where the After Action Report (AAR) indicates corrective action is warranted to improve disaster operations)
- Assist in pre-planning efforts for anticipated cascading natural hazards (secondary hazard impacts caused by the degradation from the primary hazard event)
- Be a decision-maker for their respective organization
- Have knowledge of and work within the NIMS/Incident Command System, to include the Joint Information System.
- ESF #12 Co-Lead Agencies may be asked to provide initial estimations on the energy sector impact, an anticipated restoration timeframe, areas affected by the disruption, and the percentage or number of residential and business entities without services. The ERC should have a well established relationship with public and private utilities providers where secure information exchange establishes accurate situational awareness.

Establishing the EA Communications Framework

To align roles and responsibilities of government, public and private agencies, non-governmental organizations and other supporting entities with other State planning mechanisms, establishing a collaborative response framework for communications and information sharing was imperative

for the energy sector. Through the EA planning process an EA Hierarchy was developed incorporating stakeholder input. See Figure IX-1 below.

Figure IX-1 ESF #12 EA Hierarchy



Colorado Homeland Security Strategy (HSS 2008-2013)

The State’s Department of Homeland Security was recently reorganized under the Colorado Department of Public Safety. The State’s Homeland Security Strategy outlines the direction for prevention, protection, response and recovery efforts against future catastrophic incidents whether natural or deliberate. The strategy is born out of capabilities-based planning defined as; “Planning, under uncertainty, to provide capabilities suitable for a wide range of threats and hazards while working within an economic framework that necessitates prioritization and choice.” Capabilities are the means by which a mission is accomplished with a successful outcome by performing critical tasks, under specific conditions, with the goal to target higher

levels of performance. The HSS is also aligned with the National Preparedness Guidelines. This Plan identifies capability gaps relative to the energy sector as identified in the Capabilities Gap Analysis and provides potential solutions in the Mitigation Strategy of the Action Plan. They address Prevention, Response, Recovery, Mitigation and Preparedness, which are aligned with the Mission Capabilities of the HSS as identified below. The Mission Capabilities are broken down into six categories.

- Common Capabilities**
1. Planning
 2. Communications
 3. Community Preparedness and Participation
 4. Risk Management
 5. Intelligence and Information Sharing and Dissemination

- Protect - Mission Capabilities**
1. Critical Infrastructure Protection
 2. Food and Agriculture Safety and Defense
 3. Epidemiological Surveillance and Investigation
 4. Laboratory Testing

- Prevent - Mission Capabilities**
1. Information Gathering and Recognition of Indicators and Warning
 2. Intelligence Analysis and Production
 3. Counter-Terror Investigation and Law Enforcement
 4. CBRNE Detection

- Respond - Mission Capabilities**
1. On-Site Incident Management
 2. Emergency Operations Center Management
 3. Critical Resource Logistics and Distribution
 4. Volunteer Management and Donations
 5. Responder Safety and Health
 6. Emergency Public Safety and Security
 7. Animal Disease Emergency Support
 8. Environmental Health
 9. Explosive Device Response Operations
 10. Fire Incident Response Support
 11. WMD and Hazardous Materials
 12. Response and Decon
 13. Citizen Evacuation and Shelter-in-Place
 14. Isolation and Quarantine
 15. Search and Rescue
 16. Emergency Public Information and Warning
 17. Emergency Triage and Pre-Hospital Treatment
 18. Medical Surge
 19. Medical Supplies Management and Distribution
 20. Mass Prophylaxis
 21. Mass Care (Sheltering, Feeding and Related Services)
 22. Fatality Management

Recover - Mission Capabilities

1. Structural Damage Assessment
2. Restoration of Lifelines
3. Economic and Community Recovery

Capabilities-based Preparedness Process

1. Convene working groups
 2. Determine capability requirements
 3. Assess current capability levels
 4. Identify, analyze, and choose options
 5. Update plans and strategies
 6. Allocate funds
 7. Update and execute program plans
- Assess and report

Link to Colorado’s Homeland Security Strategy:

- <http://www.colorado.gov/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1191390810427&ssbinary=true>

Local Energy Assurance Plans

Six municipalities received funding for LEAP’s in Colorado; the Cities of Aurora, Denver, Lakewood, Wheat Ridge, Aspen, and Durango. Throughout the State’s EA Planning process, the Denver –Metro municipalities have been an active stakeholder in the States efforts to plan for energy assurance. Aurora and Denver have completed their plans with Lakewood and Wheat Ridge near complete. Each LEAP is unique to its own specificities, yet is aligned with the State’s overarching goals. Through intra-state collaboration regional planning opportunities have surfaced; thus, improving capability on a regional level.

The City of Ft. Collins and Colorado Springs were also stakeholders in the EA Planning process. Though their plans are for official city business, they have brought valuable information to the table for this process. The City of Ft. Collins shared the pros and cons of a Smart Meter program piloted in their city and Colorado Springs participated in the Cyber Security workshop and exercise providing a cyber security working group opportunity to EA stakeholders.

Summary

Since September 11, 2001, civil defense and emergency management concepts have forever changed. The realization of acts of terror on domestic soil forced introspection of disaster operations from the top down and bottom up. The full extent of impacts from 9/11 may never be realized. Terrorism, whether domestic or foreign, is intentional violence or other harmful acts committed or threatened against civilians for political or ideological goals. The development of

the Department of Homeland Security is a concerted effort to prevent and disrupt such attacks. From a National perspective, every sector of society was in need of improved protective measures. As standards were mandated through Homeland Security Presidential Directives, America began a long process to change its mode of operation in response to disasters, both human-caused and natural. This complex endeavor required shared responsibility by all partners.

The EA initiative gave focus to the energy sector with intent for states to build a “new” intra-state framework for handling energy emergencies such as cyber attacks, major system outages, and threats to critical energy infrastructure and key resources statewide. By strengthening and expanding state and local government collaboration with energy sector stakeholders in energy assurance planning and resiliency efforts; and by incorporating response actions for new and existing bulk energy electric facilities, states could build in-house energy assurance expertise, thus, create jobs.

Colorado’s power of collaboration among stakeholders and the integration of standardized processes linked strategies together providing a structure that will improve overall capability regionally. Its many existing planning mechanisms support the purpose and mission of improving capability. These mechanisms were reviewed and analyzed for applicability to the EA strategy. Energy industry leaders in collaboration with local, state and federal partners have, in fact, built a regional lattice that interestingly mirrors the reliability of the power grid itself.

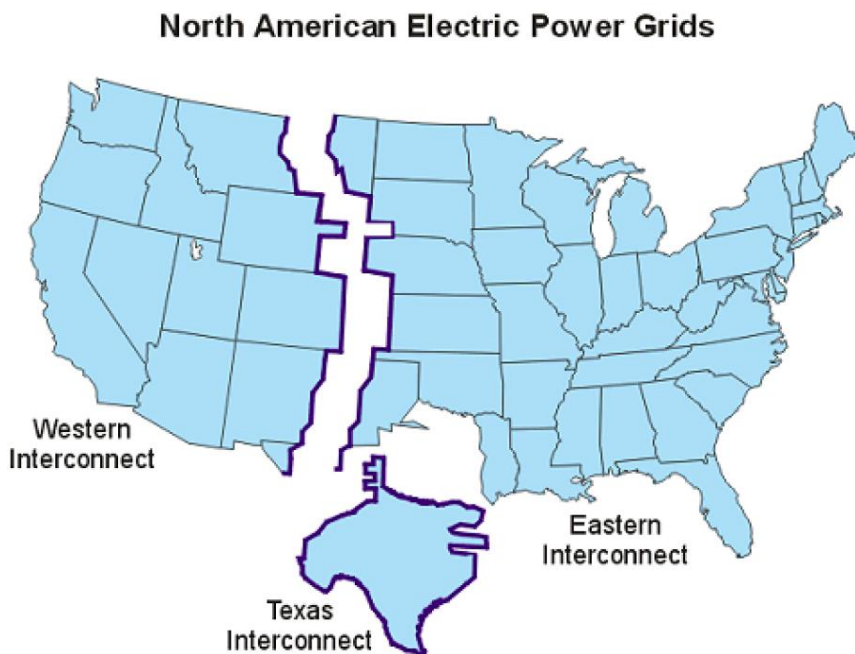
Energy Sector Profile

US and Colorado Electric Power Systems

US Electric Grid

In the US, there are three independent grids, the Western interconnect, the Eastern interconnect, and one that encompasses most of the state of Texas. Colorado is one of 11 states in the Western interconnect. Altogether in the US, there is more than 986,000 Megawatts of generation capacity as well as 275,000 miles of transmission lines.

Figure IX-2 North America Electric Power Grids



Independently, each of the three grids maintains its system frequency of 60 Hz, with a small deviation of ± 0.1 Hz. The use of alternating current (AC) was chosen over direct current (DC) in the early 20th century to be the standard way of generating, transmitting, distributing, and consuming electricity.

As power losses are proportional to the current squared, it is advantageous to increase voltage to minimize losses. From the point of electrical generation at a power plant, the electricity is stepped-up with the use of a transformer to transmission levels (115 kV to 765 kV). Often, the transmission system moves power over hundreds and even thousands of miles. It is precisely this transmission system that conjures the image of “the grid”.

To serve customer’s electrical needs, each distribution utility purchases power that is delivered to a distribution substation. The electricity is then stepped-down from the transmission level

voltage to distribution levels (e.g. 9.6 kV to 13.2 kV). The goal is still to keep the current low (which means increasing the voltage) while still minimizing the cost of the transformers that are distributed near the point of consumption. The point of demarcation between the utility's responsibility and the consumer's is the electrical meter. Typical uses of the majority of electricity are climate control, refrigeration, lighting, and plug loads (devices plugged into the sockets).

Due to the nature of electricity, the same amount of generation plus losses must equal the instantaneous consumption. All the while, the nominal system frequency of 60 Hz is necessary to maintain. Just by measuring the line frequency at any location in the grid, one can determine if the amount of electricity generated equals consumption. If the frequency is greater than 60 Hz, there is more generation than consumption. Similarly, for any measurement of less than 60 Hz, there is not enough generation than consumption.

On a nationwide scale, the US consumes 38.89 quadrillion BTUs to generate 14.28 quadrillion BTUs of electricity. Due to energy conversion processes, only 36.7% of the thermal energy is converted to electricity whereas 63.3% of the energy is lost to thermal conversion losses. Electrical generators consume 2.0% of the raw energy and another 2.5% of the energy is lost in the transmission and distribution system. That is, once electricity is produced, 5.5% is consumed by the plants themselves and another 7.4% is lost in the T&D system.

12.77 Quadrillion BTUs, equivalent to 3742 TWh, is delivered for electrical consumption. Electrical system-wide efficiency is 32.8%, measured between the generating plant and the electricity meter. There is a potential to dramatically increase system wide efficiency with the use of renewable generation. In particular, there are no thermal losses with energy conversion from wind and photovoltaics. Also, if the generation is on-site, there are no T&D losses, saving an average of 7.4% of the electricity. On an annual basis, wind and PV plants do not consume much power themselves, inclusive of when they are not generating electricity.

Colorado Electric Grid

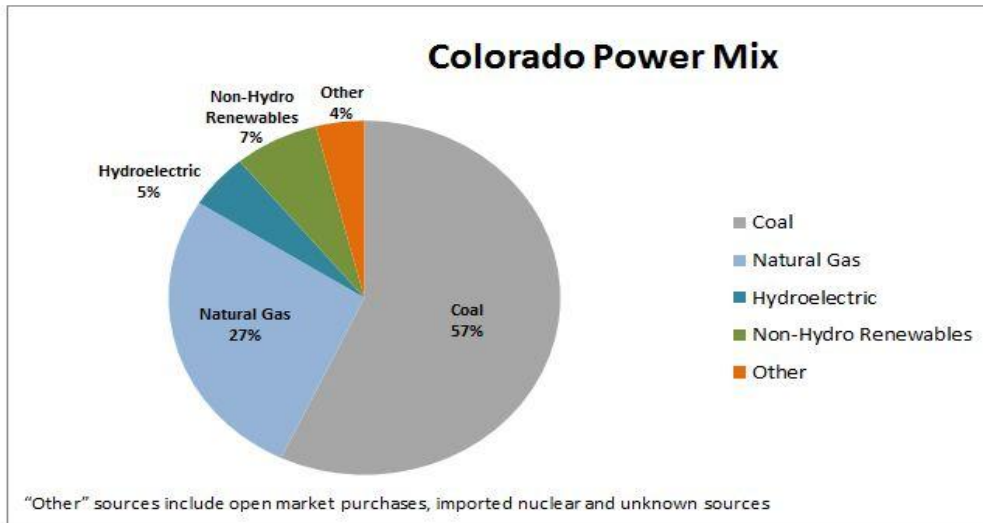
Colorado commercial and residential customers are served by a combination of investor-, municipal- and cooperatively-owned utilities:

- **Investor Owned Utilities (IOUs):** Colorado is served by two vertically integrated utilities (i.e., companies that provide bundled generation, transmission, and retail distribution services), which are regulated by the Public Utilities Commission (PUC) that sets rates and operating requirements. Public Service of Colorado (PSCO) is a Colorado subsidiary of XCEL Energy, which is a large Minneapolis-based holding company with utility operations in a number of states. It provides electrical service statewide to some 1.4 million customers and natural gas service to 1.3 million customers, accounting for over 60% of state consumption. Black Hills Energy is a smaller vertically integrated utility operating in South East Colorado, providing gas and electric service to 54 cities, accounting for approximately

1-2% of state consumption. These IOUs generate much of their own power but also supply and purchase power to and from the wholesale bulk power grid.

- Municipal Utilities:** Colorado has 29 utilities owned and operated by local government agencies. The local municipal utilities are not governed by the PUC and are responsible for setting their own rates and for their internal operating policies. They generate some of their own power and purchase the rest from the bulk wholesale market. The largest municipal utilities are in Colorado Springs, Fort Collins and Longmont, serving nearly 300,000 customers. The remaining 26 municipal utilities range in size between 201 (Fleming Electric Light Department) and 30,911 (Loveland Water and Power) customers. In total these municipal utilities serve about 403,000 customers, accounting for around 18% of state consumption.
- Cooperatives (“Co-ops”):** Colorado has 26 non-profit rural electric associations owned by their members. The Co-ops also set their own rates and are not controlled by the PUC. These smaller utilities receive most of their power from Tri-State Generation and Distribution Association (“Tri-State”), a special purpose non-profit company created and owned by its 44 members in four states to provide generation and transmission services to its member co-ops. The Co-ops serve over 1 million customers in Colorado, accounting for 21.8% of state consumption. The chart in Figure IX-3 indicates ratio of power mix for Colorado currently.

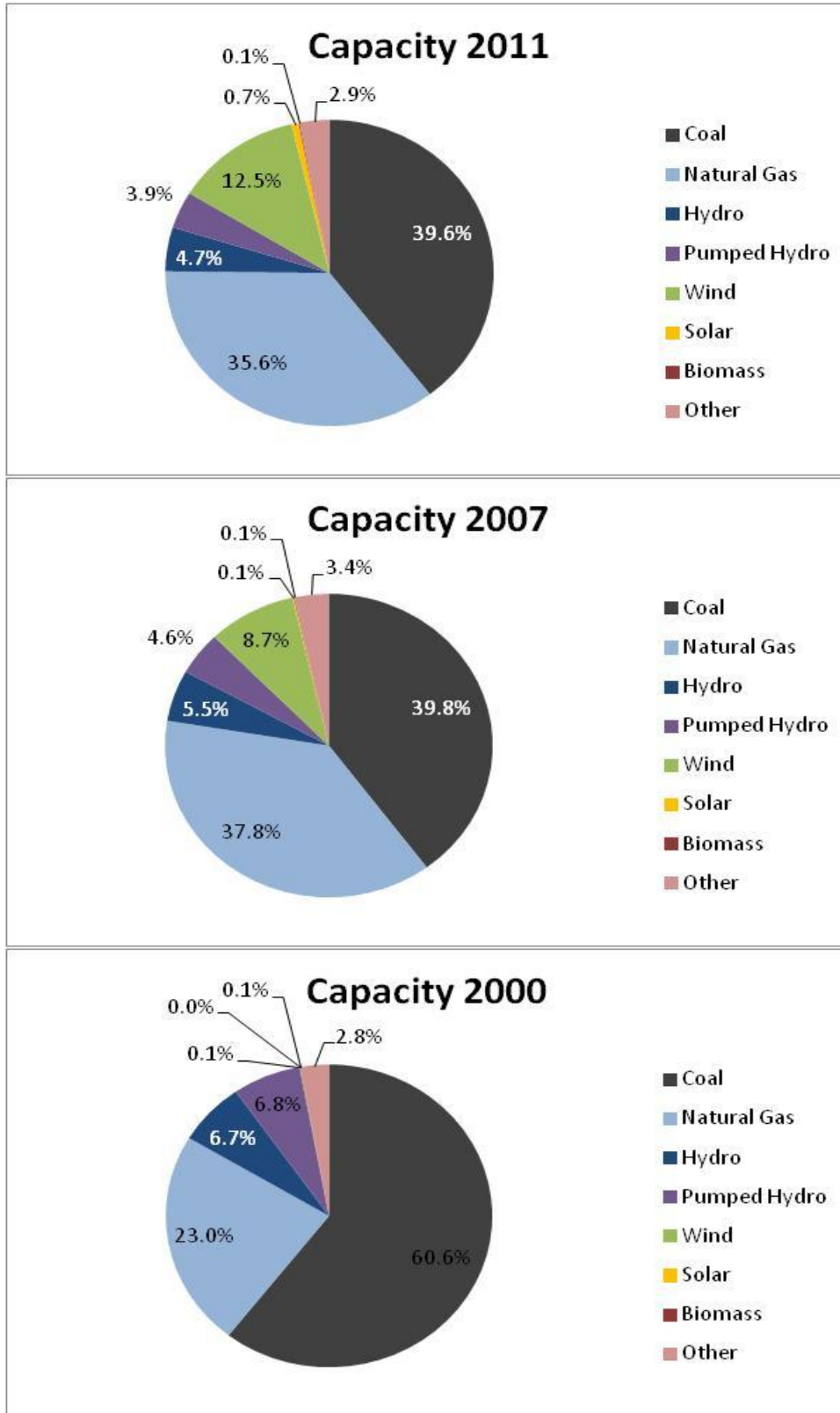
Figure IX-3 Colorado Power Mix



The electric grid is a complex network that relies on generation from a number of companies, fuel sources and locations. Currently, roughly 57% of Colorado’s power comes from coal-fired plants, 27% from gas-fired plants, 5% from hydro-electricity, 7% from wind, solar, and geothermal, and 4% from other sources (open market purchases, imported nuclear power, and other unknown resources).

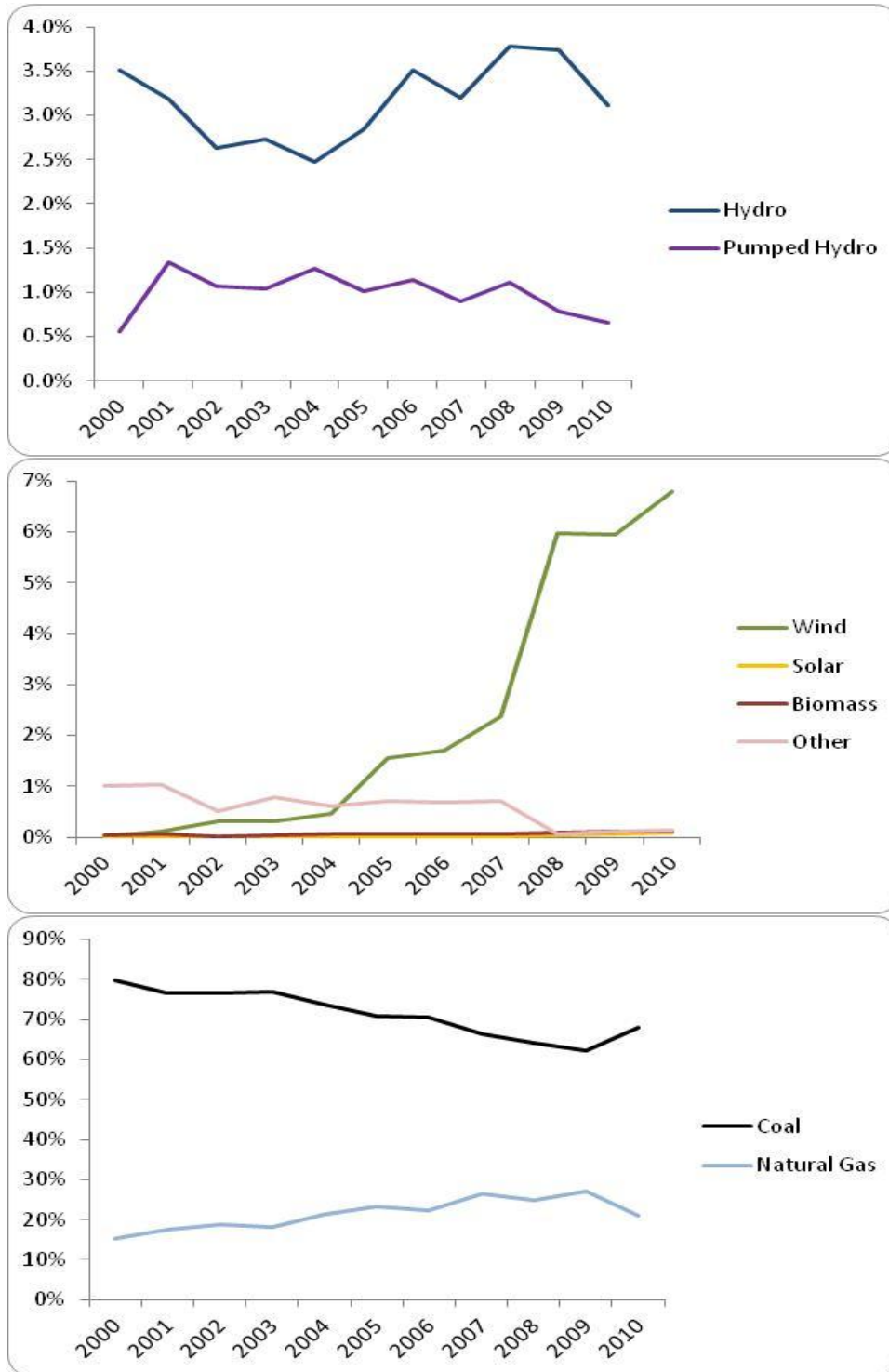
Capacity is a measure of how much electricity a generator can produce under specific conditions. **Generation** is how much electricity a generator produces over a specific period of time. For example, a generator with 1 MegaWatt (MW) capacity that operates at that capacity consistently for one hour will produce 1 MW-hour (MWh) of electricity. If it operates at only half that capacity for one hour, it will produce 0.5 MWh of electricity. Many generators do not operate at their full capacity all the time; they may vary their output according to conditions at the power plant, fuel costs, and/or as instructed from the electric power grid operator. **Net generation** is the amount of gross generation less the electricity used by the generating station/power plant to operate the plant, including fuel handling, boiler and cooling water pumps, pollution control equipment, plant lighting, and computers. In Figure IX-4 note the rate of change in Capacity between the year 2000 and 2007. Capacity for 2011 is relatively the same as 2007.

Figure IX-4 Difference in Capacity from 2000-2011



Note in the line graphs in Figure IX-5 the rate of change in generation from the different sources over time.

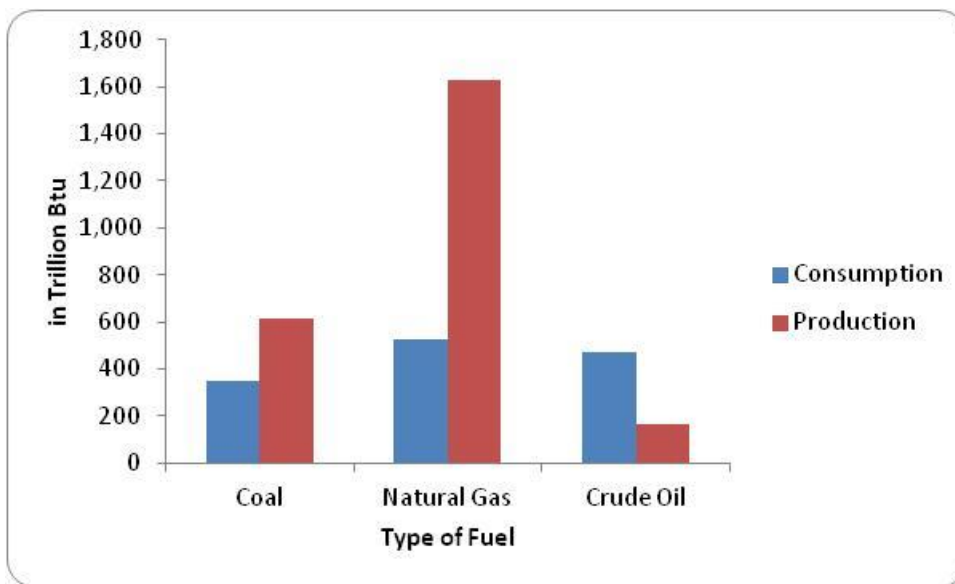
Figure IX-5 Rate of Change in Generation 2000-2010



Generating plants produce alternating current at medium voltages, which is then increased by step-up transformers for transport on high-voltage bulk power “transmission” lines. Closer to the point of use, the high voltage electricity is stepped down at medium voltage substations, and then further stepped down to low voltage “distribution” lines that feed commercial and residential users. Most renewable energy plants (e.g., wind and solar) produce direct current electricity, which has to be converted to alternating current before it can be fed into the grid.

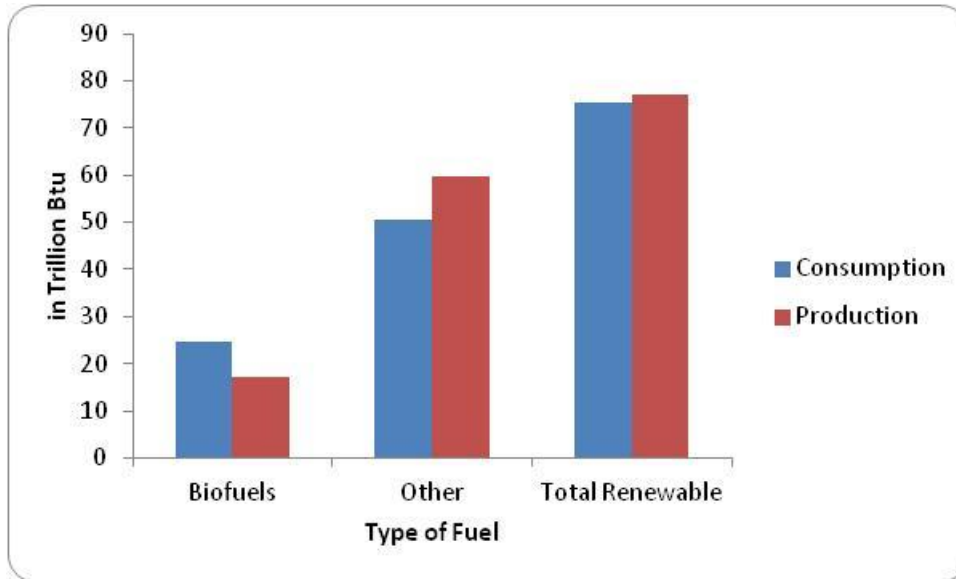
Colorado produced roughly 2,483 trillion Btu of energy in 2010 and consumed approximately 1,452 trillion Btu, or 58% of that total. Therefore the state theoretically has considerable excess generating capacity to meet potential emergencies, although as a practical matter, transmission constraints, operating agreements, and actions by balancing authorities may significantly limit flexibility to divert capacity to specific areas in Colorado under various emergencies. In Figure IX-6 below, the bar graph indicates the difference between fossil fuel energy fuel production and consumption. The excess is not necessarily exported.

Figure IX-6 Fossil Fuels: Production vs. Consumption - 2009 Colorado Fossil Fuels Energy Production versus Consumption Estimates



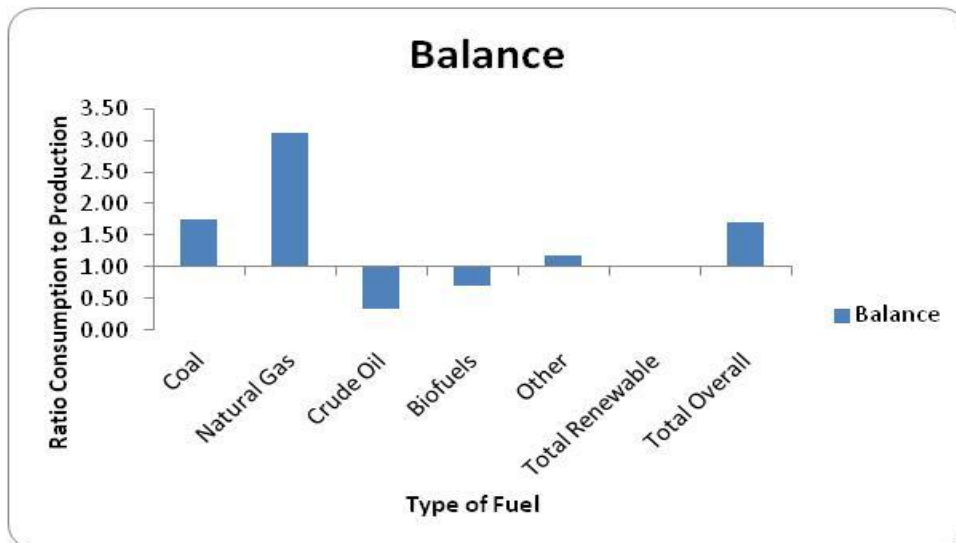
In Figure IX-7 below, the bar graph indicates the difference between renewable energy fuel production and consumption. Again, the excess is not necessarily exported.

Figure IX-7 Renewable Energy: Production vs. Consumption - 2009 Colorado Renewable Energy Production versus Consumption Estimates



In Figure IX-8 below, the bar graph indicates the balance between production and consumption of all fuels. The bars that are pointing upward (above 1) indicate that Colorado produces more than it consumes. The bars that are pointing downward (below 1) indicate that Colorado consumes more than it produces. The total consumption versus production would be at about the 2.5 mark.

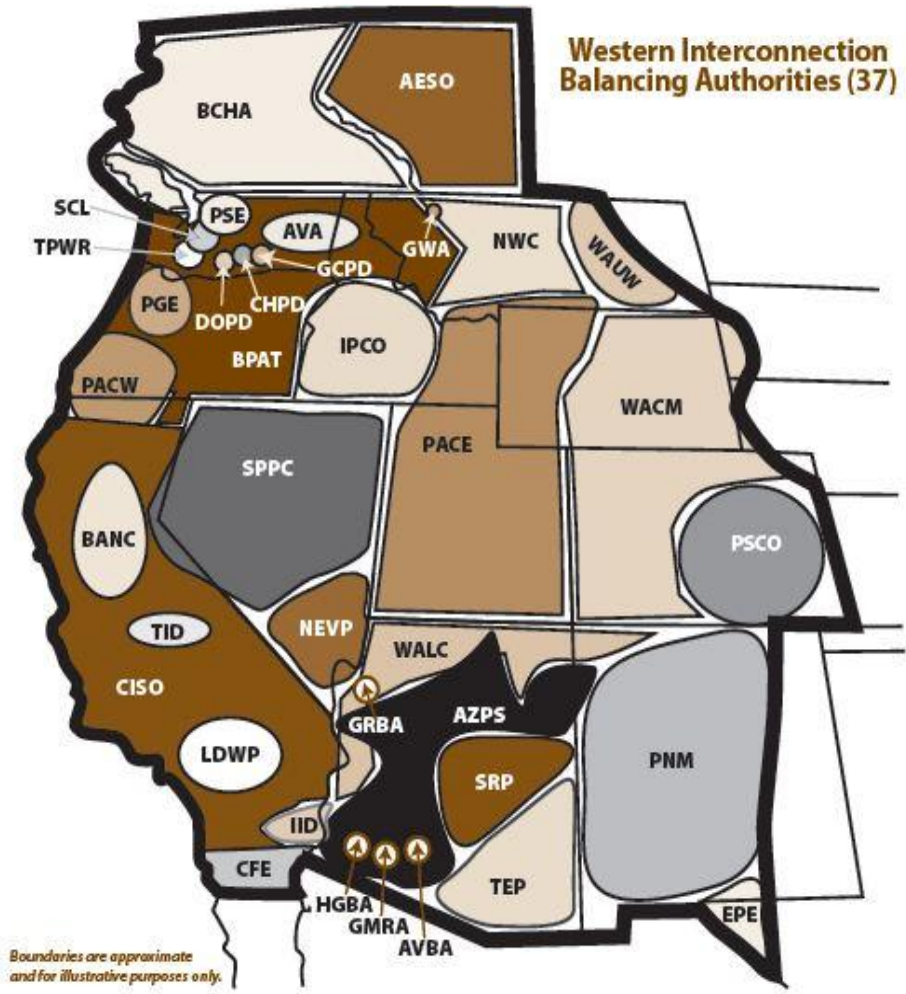
Figure IX-8 Colorado Balance: Production vs. Consumption - 2009 Colorado Balance of Production versus Consumption Estimates



The grid has to produce exactly the amount of power that is consumed at any moment in time in order to maintain voltages and frequency. If voltages exceed very narrow ranges, equipment can be damaged and the system can collapse as key components automatically trip off protectively. In order to maintain the delicate balance between demand and supply in the system, the United States is divided into three essentially separate regions. Colorado is part of the Western Electric Coordinating Council (WECC) inter-connection region. WECC is a voluntary association of utilities that coordinates utility planning and the real-time actions necessary to maintain reliability of the bulk grid. It covers all of the western states, two Canadian provinces, and the northern part of Baja California, Mexico.

The western interconnection under the WECC area is further divided into regional “balancing authority” areas, with PSCO being the balancing authority for much of Colorado, with responsibility for maintaining generating balance and real-time interconnection frequency among the various generators and users in the region. The Western Area Power Administration Colorado-Missouri Region (WACM) is one of four power marketing administrations in the United States. The WACM markets and delivers hydroelectric and other services within a 15 state region of the western and central U.S. In the event of a systems-wide collapse, each of these regional areas will separate as the system protects itself and then begins to reconnect to restore power in shut-down areas as the utilities bring generation back on line under so-called “black start” conditions. WECC operates under national level standards set by the North American Electric Reliability Corporation (NERC), which is the reliability organization designated to establish and enforce the reliability standards set by the Federal Electric Regulatory Commission (FERC) for the bulk power system.

Figure IX-9 Western Interconnection Balancing Authorities

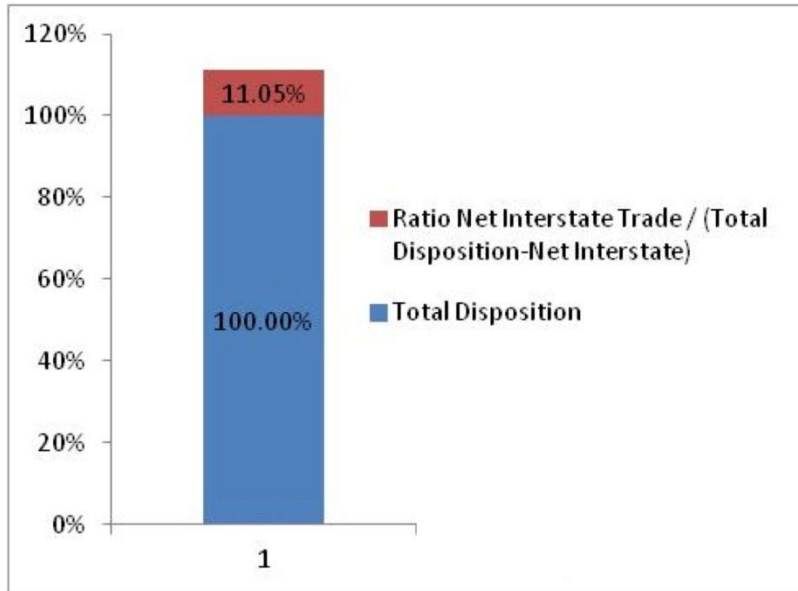


- | | |
|--|--|
| <p>AESO: Albert Electric System Operator
 AVA: Avista Corporation
 AVBA: Arlington Valley, LLC*
 AZPS: Arizona Public Service Company
 BANC: Balancing Authority of Northern California
 BPAT: Bonneville Power Administration-Transmission
 BCHA: British Columbia Hydro Authority
 CFE: Commission Federal de Electricidad
 CHPD: PUD No. 1 of Chelan County
 CISO: California Independent System Operator
 DOPD: PUD No. 1 of Douglas County
 East PACE: PacifiCorp
 EPE: El Paso Electric Company
 GCPD: PUD No. 2 of Grant County
 GRBA: Griffith Energy, LLC*
 GRMA: Gila River Power, LP*
 GWA: NatuEner Power Watch LLC*
 HGBA: New Harquahala Generating Company
 IID: Imperial Irrigation District
 IPCO: Idaho Power Company
 LDWP: Los Angeles Department of Power and Water
 NWC: North Western Energy
 PGE: Portland General Electric Company</p> | <p>PNM: Public Service Company of New Mexico
 PSCO: Public Service Company of Colorado
 PSE: Puget Sound Energy
 SCL: Seattle City Light
 SRP: Salt River Project
 SPPC: Sierra Pacific Power Company
 TEP: Tucson Electric Power Company
 TID: Turlock Irrigation District
 TPWR: City of Tacoma, Department of Public Utilities
 WACM: Western Area Power Administration, Colorado-Missouri Region
 WALC: Western Area Power Administration, Lower Colorado Region
 WAUW: Western Area Power Administration, Upper Great Plains West
 West PACE: PacifiCorp
 *Generation-only, controls no load</p> |
|--|--|

Colorado Electricity Imports/Exports

Net Interstate Trade is the net of imports and exports, which for Colorado is 6,302 thousand MWh in imports. This indicates that Colorado receives approximately 11% of its distribution from out of state.

Figure IX-10 Ratio Net Interstate Trade



Colorado Grid System Risks

The risks of energy emergencies differ substantially in the different parts of Colorado’s electricity system.

- **Generation:** Given the surplus of generating capacity, the risks from loss of any given generating plant are relatively low. The system is designed to manage both planned outages (e.g., for routine maintenance) and emergencies where the system has to be able to manage the unanticipated loss of the most critical parts of the system. It can presumably manage the loss of any single component without problem. The biggest threats to the system therefore are the loss of multiple generating sources at the same time, most likely from a low probability event like cyber attacks, terrorist action, or possibly a major geomagnetic storm that knocked out step-up transformers at the generating stations. Serious damage to generating stations would lead to prolonged recovery periods.
- **Transmission:** Loss of multiple extra high voltage transformers would have a major impact on ability to deliver power to large areas in Colorado, as the lead time for replacement is a year or more. Again the primary risk of this scenario would be cyber or terrorist attack or a major geomagnetic storm that knocked out extra high voltage transformers. There is, however, some disagreement as to the vulnerability of Colorado’s bulk transmission system from geomagnetic events because of our lower latitude, geology, and the fact that the highest voltage bulk transmission lines in Colorado are only 345kv, while the greatest risk is to lines of 500kv or above, which are predominantly in the Northeast and Northwest of the country.
- **Distribution:** Distribution is the most vulnerable portion of the electricity system as above-ground local lines are especially susceptible to weather events. The local distribution infrastructure, however, is generally able to be restored fairly quickly (i.e., in hours or a few days) as long as there is access to the area. Utilities have well-developed and exercised plans for quick restoration, including mutual aid pacts to provide skilled labor from sister utilities as needed. Table IX-1 below lists the 10 top power plants in Colorado in 2010 by generating capacity. The scatter graph in Figure IX-11 below the table indicates the comparison.

Table IX-1 Colorado Top Ten Power Plants

Top Ten Power Plants in Colorado 2010 (by generating capacity)			
Plant	Resource	Operating Company	Net Summer Capacity (MW)
1. Comanche	Coal	Public Service Co of Colorado	1,426
2. Craig	Coal	Tri-State G&T Association, Inc.	1,304
3. Fort St. Vrain	Gas	Public Service Co of Colorado	969
4. Cherokee	Coal	Public Service Co of Colorado	717
5. Rawhide	Coal	Platte River Power Authority	666
6. Rocky Mountain Energy Center	Gas	Rocky Mountain Energy Ctr. LLC	601
7. Pawnee	Coal	Public Service Co of Colorado	505
8. Front Range Power Project	Gas	City of Colorado Springs	462
9. Hayden	Coal	Public Service Co of Colorado	446
10. Cabin Creek	Pumped Storage	Public Service Co of Colorado	324

Figure IX-11 Scatter Graph Plotting the Top Ten Power Plants in Table IX-1 above.

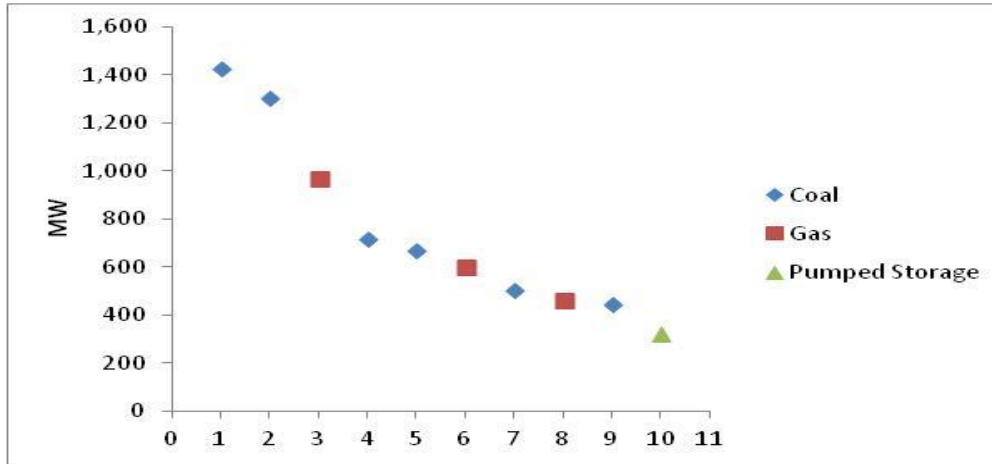
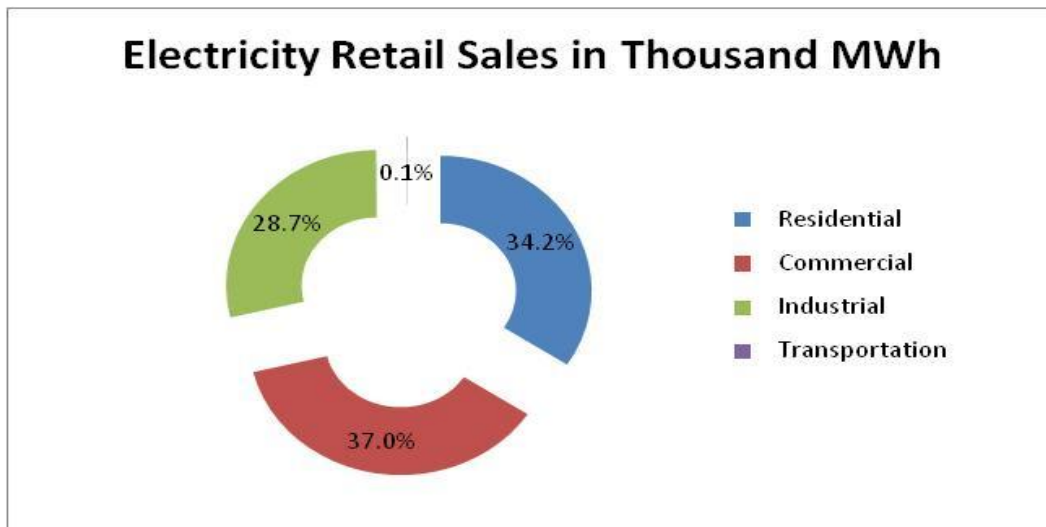


Figure IX-12 Colorado 2010 Electricity Retail Sales by Sector



Trends in the Industry

The current electric grid is currently very much a one-way, top down system from the utilities to the customers. Customers are passive receivers of electricity and the utilities have minimal ability to reduce demand when supplies are tight (except for limited interruptible contracts with selected commercial and industrial customers). Moreover, the transmission system has been increasingly stretched thin as demand for power goes up and not-in-my-backyard resistance prevents construction of new transmission lines. As a result, the bulk transmission system is becoming increasingly strained and lots of attention is currently being paid to ways to make it more flexible and robust. Fortunately several mutually reinforcing trends offer the potential to dramatically improve the situation over the next decade or so.

- **Distributed Generation Opportunities:** Current thermal generation technologies (whether coal, natural gas, or nuclear powered) have tremendous economies of scale and have pushed the industry to larger central generating stations. The emergence, however, of renewable energy technologies, which has grown significantly in Colorado over the past five years, along with other smaller-scale applications, such as combined heat and power (CHP) units are making it cost-effective to locate smaller generators closer to end users. These “distributed generation” opportunities can limit the need for building new long-distance, high voltage transmission lines and the vulnerabilities associated with them. In addition, with the emergence of smart grid technologies, distributed generation facilities will have the ability to isolate (“island”) themselves from the bulk grid and to continue to operate during energy emergencies.
 - While the near-term prospects for distributed generation are difficult to predict, solar will almost certainly be the primary technology as panel prices continue to fall dramatically. It is likely that utilities will start supporting medium size distributed solar investments (1 to 10 MW) range and then the growth will expand to residential systems in the kilowatt range. Utilities will presumably be able to integrate mid-size renewable projects that they or independent power producers (IPPs) develop into the grid relatively easily. The ability to use residential scale projects for enhancing grid stability, however, will clearly depend on the deployment of sophisticated smart grid technologies.
- **Smart Grid Technologies:** Smart grid technologies are key to taking full advantage of renewable energy technologies and distributed generation opportunities. Additionally, smart grid technology allows for a more efficient management of existing resources and provides more rapid and intelligent prevention and response to energy disruptions. With the current centralized utility system, most commercial and industrial facilities lack the ability to protect themselves and generate their own electricity, except through back-up diesel generators (which themselves are at risk of running out of fuel after a few days if retail gas stations cannot pump fuel because of electric outages). Current residential owners cannot use their solar systems during outages (unless they have backup battery storage and can isolate themselves from the grid) because of utility procedures to protect linemen while restoring power.
 - The smart grid technologies necessary to allow homeowners (and most other commercial establishments with their own renewable generation systems) to operate during outages are only now being developed. It is likely, however, that within the next few years, the technologies to allow this kind of independent operation will be commercialized. Smart meters will allow utilities to identify, work-around, and correct outages much more quickly. One additional possibility of smart grid technology would be innovative rate structures that integrate time-of-use electric rates over the course of the day based on fluctuating “demand charges” by the utilities. This ability for consumers to adjust their use to minimize electricity costs will become especially appealing when combined with electric vehicles that can store electricity and feed it back to the grid when the utilities are willing to pay to meet peak power demands.

- **Electric Vehicles:** Vehicle-to-grid (V2G) technologies allow electric vehicles to either accept power to charge or sell power back to the grid. The number of electric vehicles is currently far too small to be a significant factor and the electronics to manage these vehicle-to-grid systems are still in their infancy. But the average car is sitting still for over 22 hours a day, when it could be charging when demand is low or providing power back to the grid when peaking power is needed. With appropriate metering, if the grid goes down, key appliances in the house could be run off the batteries in the car during an energy outage, thereby adding considerable resiliency to the system. When combined with solar panels on the roof, this ability to either feed power to the grid when needed or isolate from the grid and rely on self-generation when prices are high, provides even greater grid efficiency and protection against service disruptions.
- **Micro-grids:** A micro-grid is a small, localized grouping of electricity generation and storage that can operate either independently or as connected to the larger, centralized grid (the macro-grid). Micro-grids or “mini-grids” have the ability to generate much of their own required power and can elect when they acquire power from the bulk wholesale market. More importantly, from an energy assurance perspective, micro-grids will be able to isolate (“island”) themselves during an energy emergency or outage and continue to meet the basic needs of their owners or customer base. The U.S. military (Fort Carson is one of the beta sites) is leading the way in developing these types of micro-grids, emphasizing renewable sources, because of their awareness of fossil fuel dependencies and vulnerabilities of the bulk power system to disruption. Other likely leaders in the shift to micro-grids are universities and industrial facilities that tend to be early adopters or have a particular need for uninterrupted, high quality power.

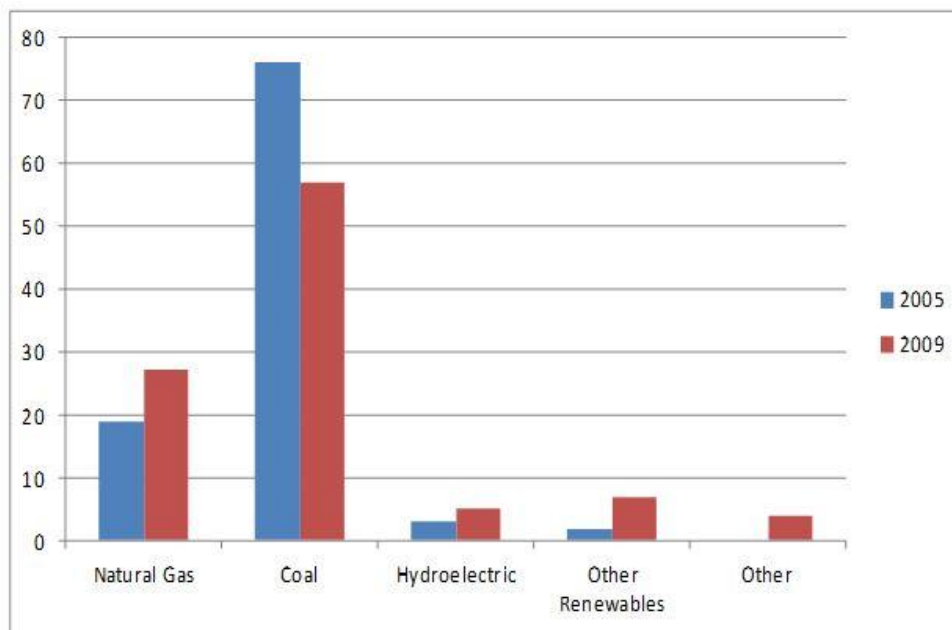
Colorado Energy Resource Profiles

The following five sections provide a brief overview of resource production, consumption, and infrastructure in Colorado. This general summary is designed to provide a basic background on Colorado’s energy resources to support stakeholder decision making in planning, mitigation, response, and recovery.

Natural Gas

Demand for natural gas in the United States has exceeded supply for most of the decade. Although natural gas is relatively cost-effective at today’s market prices, the supply chain takes years to develop.

Figure IX-13 Colorado Electric Power Mix, 2005 and 2009



Source: 2010 Electric Utilities Report and US Department of Energy EERE Report

Colorado is a top natural gas producing state and has constructed a complex network of natural gas infrastructure. According to the U.S. Energy Information Administration, Colorado basins account for more than 5% of U.S. natural gas production and the state is home to ten of the nation’s largest natural gas fields.

Coalbed methane production in Colorado accounts for over 40% of all coalbed methane produced in the United States with the Piceance Basin in Northwest Colorado holding the second-largest reserve in the nation.

Table IX-2 Natural Gas Consumption by End Use

Show Data By:		2005	2006	2007	2008	2009	2010	View History
<input checked="" type="radio"/> Data Series	<input type="radio"/> Area							
Total Consumption		470,321	450,832	504,775	504,783	520,206		1997-2009
Lease and Plant Fuel								1967-1998
Lease Fuel		35,866	38,088	39,347	44,231	64,873		1983-2009
Plant Fuel		15,641	16,347	16,218	18,613	21,288		1983-2009
Pipeline & Distribution Use		13,305	12,945	13,850	15,906	13,659		1997-2009
Volumes Delivered to Consumers		405,343	383,307	435,219	425,913	420,249	NA	1997-2010
Residential		124,255	119,270	130,971	133,947	128,993	132,900	1967-2010
Commercial		62,099	59,851	63,231	65,806	62,441	NA	1967-2010
Industrial		126,360	111,259	117,230	119,706	113,582	113,997	1997-2010
Vehicle Fuel		166	144	141	121	136	153	1988-2010
Electric Power		92,629	92,927	123,788	106,454	115,234	94,291	1997-2010

Source: Energy Information Administration, 2012

Colorado uses only about two-fifths of its natural gas production while the remaining supply is exported to markets primarily through corridors servicing the Western and Midwestern United States.

The economic viability of natural gas coupled with existing infrastructure and geographic proximity to natural gas supplies has increased natural gas consumption by the electric power sector in Colorado over the past decade. In recent years, the electric power sector has become a major consumer of natural gas, second only to residential users and occasionally, industrial consumers. By 2009, 27% of Colorado’s electric power was produced by natural gas power plants.

Natural Gas Production and Infrastructure

Natural gas is extracted from oil fields (associated), isolated natural gas fields (non-associated), and coal beds (coalbed methane). The gas that is extracted directly from the wellhead contains a mixture of various chemical gases and requires processing to remove impurities. The final product that we call “natural gas” is actually a pure form of methane gas. Historically, natural gas was viewed as an inconvenient by-product of petroleum production. Without pipelines to transport gas to end-users, the excess gas was simply burned off at the oil field. In the past fifty years, however, natural gas infrastructure has spread throughout the country and the resource itself has gained a reputation as a cleaner burning alternative to other hydrocarbon fuels.

The number of natural gas producing wells in the state of Colorado has increased from 16,718 in 2004 to 27,021 in 2009. Consequently, Colorado is home to over 5% of the total natural gas producing wells in the entire nation. With over 11 major interstate pipelines, 22 natural gas fired-generators, and thousands of natural gas producing wells, Colorado has established an intricate natural gas network. The complexity of the natural gas infrastructure increases efficiency and reliability under normal operating conditions, but interdependencies embedded in the system can also increase vulnerability to disruption.

Extracting, transporting, and processing natural gas for consumption requires a sophisticated network of physical transfers and processing steps. The infrastructure designed to complete the transfer of gas from the wellhead to the user can be illustrated more clearly by defining the major physical facilities and technologies employed in natural gas production and transportation.

Natural Gas Physical Facilities and Systems

Gathering Lines:

Small pipelines that move natural gas from the wellhead to the natural gas processing plant or to an interconnection with a larger mainline pipeline

Processing Plant:

Facilities that extract liquids and impurities from the primary natural gas stream

Mainline Transmission Systems:

Long-distance/wide-diameter pipelines that transport natural gas from producing areas to market areas

Compressor Units:

Compressor stations, located along the transmission system, increase the pressure and rate of natural gas flow in order to maintain the movement of gas along the pipeline

Market Hubs/Centers:

Locations where pipelines intersect and flows are transferred

Underground Storage Facilities:

Natural gas is stored in depleted oil and gas reservoirs, aquifers, and salt caverns for future use

LNG Peaking Facility:

A facility or system that allows natural gas providers to meet short-term surges in demand; liquid gas such as propane is vaporized and injected into the natural gas stream

SCADA:

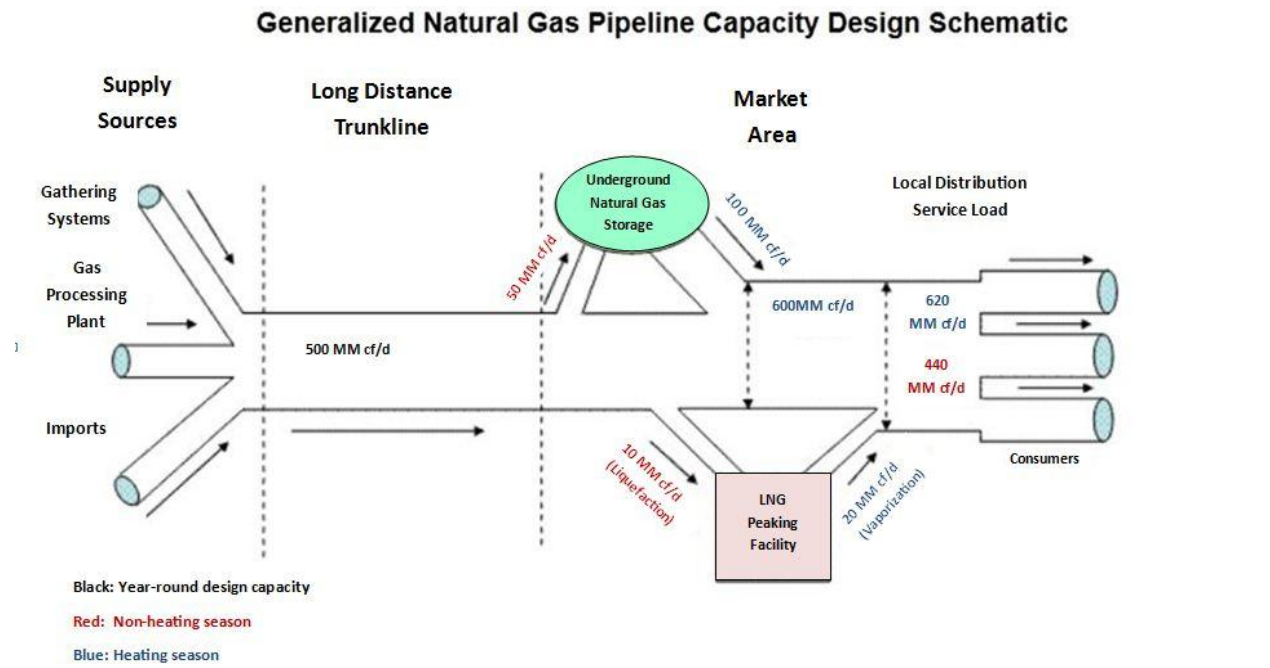
Systems Control and Data Acquisition systems provide real-time monitoring of pipeline flow, integrity, and pressure

Safety Cutoff Meters:

Devices located along the transmission system that detect a decrease in pressure resulting from a rupture in the pipeline. If a significant decrease in pressure is detected, then these units will automatically shut down the flow of gas

Figure IX-14 below provides a diagram of an alternative view of the natural gas flow from the wellhead to the end user. Regional natural gas systems do not always follow the same route. For example, not all underground storage facilities are designed to provide peaking services (to meet short term surges in natural gas demand). If a storage facility does provide this type of service, then the local supplier must weigh the costs and benefits of constructing a redundant peaking facility. However, the financial consequence of a major service interruption may outweigh the initial investment in a peaking facility unit. In markets where dramatic seasonal or temperature extremes occur, companies may face daily or hourly fluctuations in natural gas demand. Therefore, peaking facilities may be necessary to keep the natural gas supply flowing during high demand seasons.

Figure IX-14 Natural Gas Pipeline Capacity



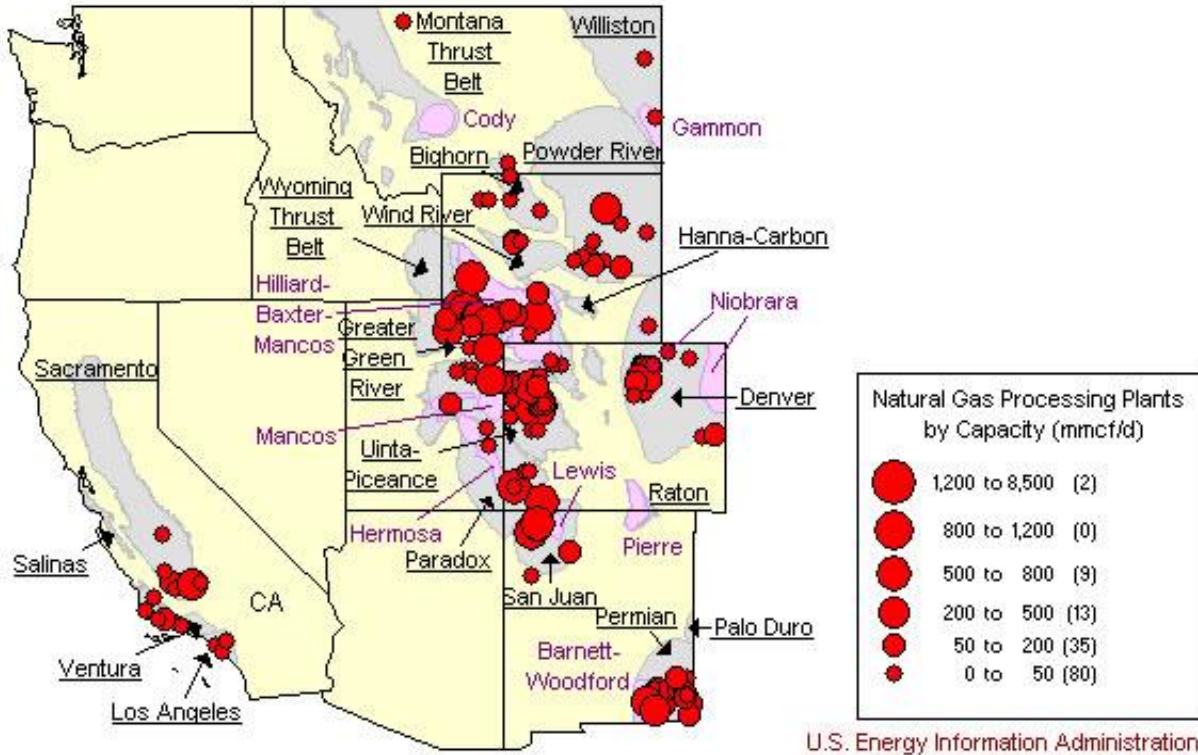
Source: EIA Generalized Natural Gas Pipeline Capacity Design Schematic, available from: http://205.254.135.7/pub/oil_gas/natural_gas/analysis_publications/ngpipeline/FlowDiagram.html

Natural Gas Processing

For the natural gas grid to operate safely, wellhead gas must be processed or cleaned to remove contaminants and natural gas liquids. Unprocessed wellhead natural gas may cause pipeline deterioration and/or rupture.

- Btu content range must lie within 1,035 Btu +/- 50 Btu
- Natural gas must be transported at a specific dew point temperature range
- Trace amounts of elements such as oxygen, nitrogen and water vapor must be removed
- Particulate solids and/or liquid water must be eliminated

Figure IX-15 Natural Gas Processing Plants



Between 2004 and 2009, processing capacity in Colorado more than doubled. Note that the largest processing plant locations coincide with the two existing natural gas market centers: the Cheyenne Hub in the Northeast and the White River Hub to the West.

Natural Gas Storage

Natural gas is stored in underground storage facilities during non-peak periods and may be released when peak demand is predicted. The state of Colorado is home to nine depleted natural gas/oil reservoir storage facilities.

Natural gas storage may provide suppliers with the means to meet peak-season natural gas demand. More commonly, liquid natural gas and liquefied petroleum are vaporized and injected into the distribution supply to meet peaking requirements. In general, storage facilities in Colorado are used to store excess production rather than to supply natural gas for local production.

Table IX-3 Colorado Natural Gas Storage Facilities

Company	Field	Reservoir	County	Working Gas Capacity (Mcf)	Total Field Capacity (Mcf)	Maximum Daily Delivery (Mcf)
Public Service Company Of Colorado	Asbury	Dakota	Mesa	3056731	4593268	10168
Sourcegas Energy Services	Wolf Creek	Cozette	Pitkin	2205695	7100000	23000
Public Service Company Of Colorado	Roundup	J Sand	Morgan	6029784	16080524	37431
Public Service Company Of Colorado	Fruita	Buckhorn	Mesa	257614	320340	N/A
Colorado Interstate Gas Company	Flank	Morrow and Cherokee	Baca	7182777	19891378	164104
Colorado Interstate Gas Company	Latigo	Dakota J	Arapahoe	9100000	22278343	139240
Colorado Interstate Gas Company	Young	Dakota D Sand	Morgan	5790049	9945689	250000
Colorado Interstate Gas Company	Fort Morgan	Dakota D	Morgan	8496000	14858000	450000
Colorado Interstate Gas Company	Totem Storage	J Sand	Adams	7000000	10700000	200000

EIA Field Level Storage Data, available from: http://www.eia.gov/cfapps/ngqs/ngqs.cfm?f_report=RP7

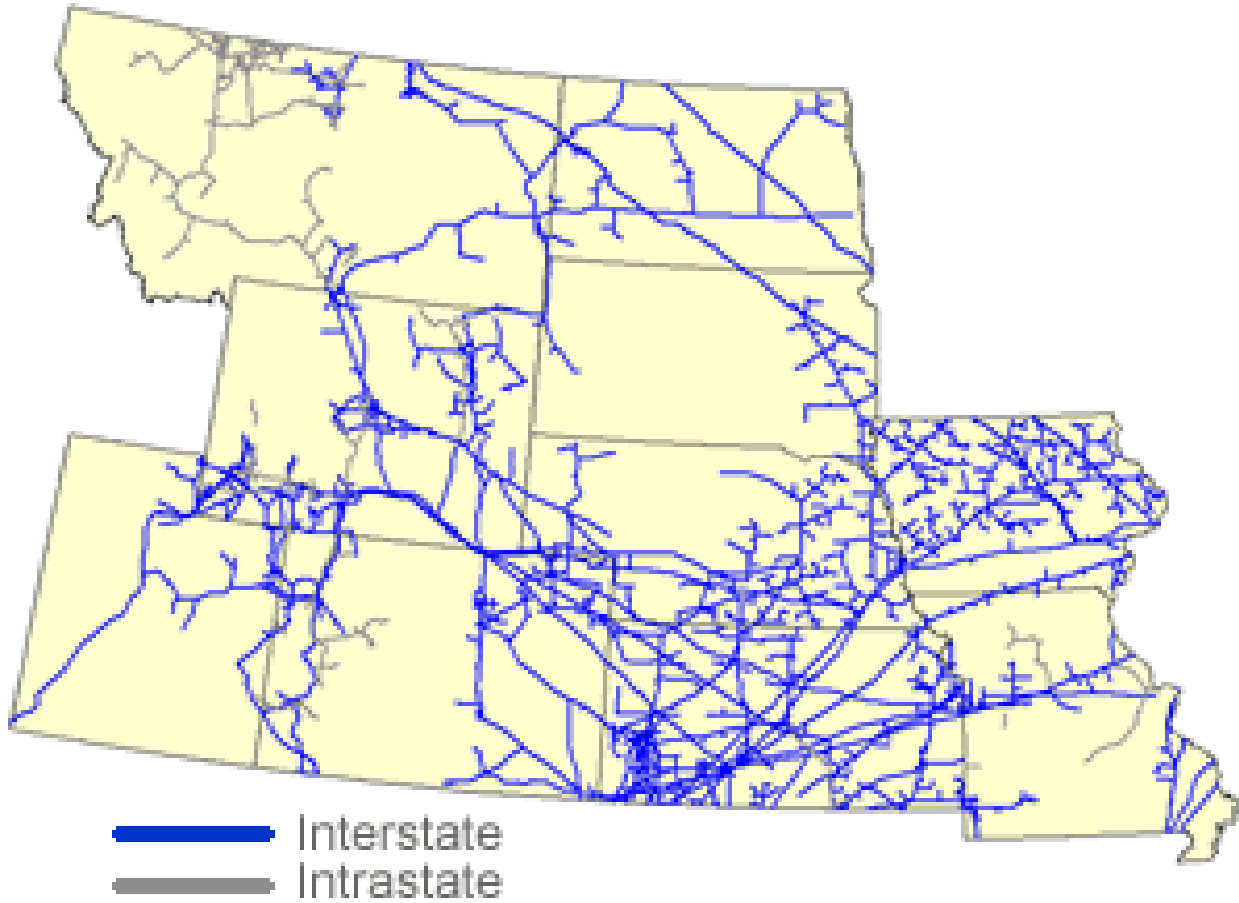
Natural Gas Pipelines, Hubs, and Local Distribution Companies

Natural gas trunk lines carry the largest capacity of natural gas over long distances, while grid systems operate and serve major market areas. Grid systems transport natural gas to local distribution companies and large volume consumers. Colorado lies in the Central natural gas corridor and is home to two natural gas market hubs and at least eleven major natural gas pipelines. Seven of the thirty largest natural gas pipeline systems pass through the state of Colorado, some of these include:

- Colorado Interstate Gas
- El Paso Natural Gas Co.
- KM Interstate Gas Co.
- Northwest Pipeline Corp.
- Panhandle Eastern Pipeline Co.
- Questar Pipeline Co.
- Rockies Express Pipeline
- Southern Star Central Gas Pipeline
- Trailblazer Pipeline Co.

- Wyoming Interstate Gas Co.
- Transwestern Pipeline Co.

Figure IX-16 Central Region Natural Gas Pipeline Network



EIA Central Region Natural Gas Pipeline Network http://www.eia.gov/pub/oil_gas/natural_gas/analysis_publications/ngpipeline/central.html

Local distribution companies transport natural gas from interstate pipeline delivery points to end users. These delivery points or “city gates” are important market centers for pricing natural gas. The Public Service Company of Colorado is the largest local distribution company in the state and receives nearly all of its supply from Colorado Interstate Gas. There are six electric utilities that provide natural gas service and eight utilities that provide only natural gas service.

Colorado Natural Gas Hubs

Natural gas market centers, or hubs, perform three basic roles in the movement and trade of natural gas:

- Provide customers with receipt and delivery access to two or more pipeline systems
- Provide transportation between these points
- Provide administrative services that facilitate the movement or transfer of gas ownership

The Cheyenne hub in Northeastern Colorado is classified as a ‘header hub’; meaning that the hub resides at the head of a major natural gas system. In other words, the Cheyenne hub is physically located next to pipeline transfer points and other facilities such as underground storage. Many of these hubs provide customers with Internet-based gas trading websites or “Information Postings”. The newest market hub is the White River Hub in Western Colorado which was created to provide access to intrastate and interstate pipelines to natural gas producers in the Piceance and Uinta Basins. The Cheyenne Hub, opened in 2000, is owned and operated by Colorado Interstate Gas Company and provides access to multiple pipelines servicing the Western and Midwestern markets.

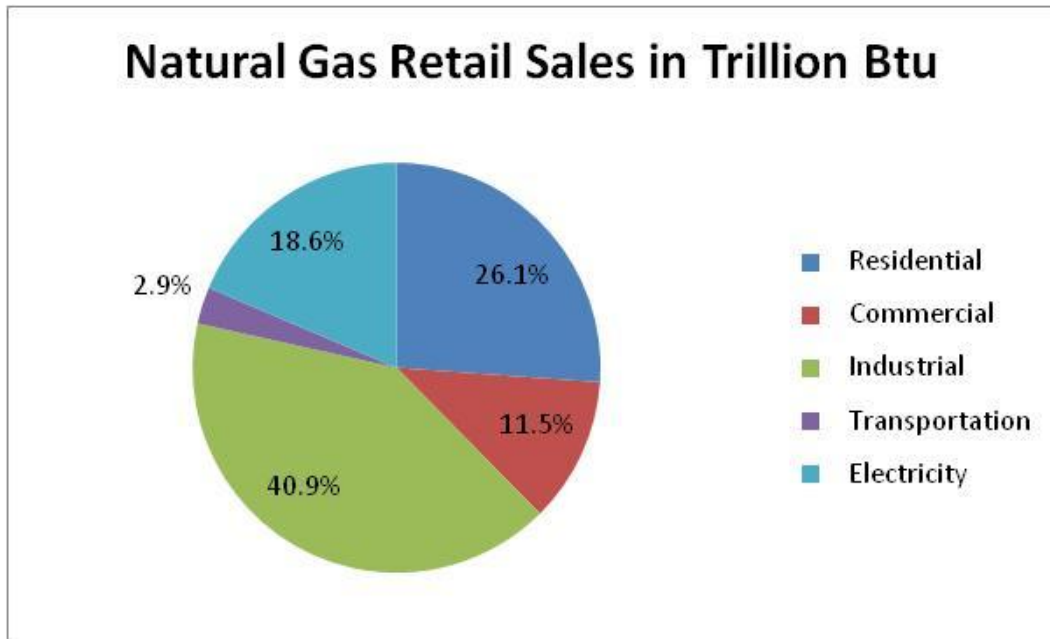
Table IX-4 Natural Gas Market Centers

	Cheyenne	White River
Administrator	Colorado Interstate Gas Co.	White River Hub LLC
Online Customer Service System	CIG-Xpress	Questor
Type of Infrastructure	Header	Header
Type of Operation	Market Hub	Production Hub
Year Started	2000	2008
Associated Processing Plant	none	Meeker
Associated Storage Site Name	Young/Ltigo/Huntsman	none

EIA Natural Gas Market Centers Update: 2008, available from:
http://www.eia.gov/pub/oil_gas/natural_gas/feature_articles/2009/ngmarketcenter/ngmarketcenter.pdf

The natural gas industry has stakeholders at both ends of the pipeline; with producers who feed gas into the system and local distributors or utilities who provide power to the end user. Natural gas outages, incidents, or emergencies carry the potential for a failure at each end of the system. Larger disruptions along major transmission lines could negatively impact the transportation options for producers. Simple residential gas leaks could affect local consumption. Natural gas electric utilities depend on an uninterrupted supply of fuel to keep the turbines running; while market centers rely on both consumers and producers to manage supply and delivery. All of these systems are dependent on one another and are intricately tied to the Colorado energy sector as a whole.

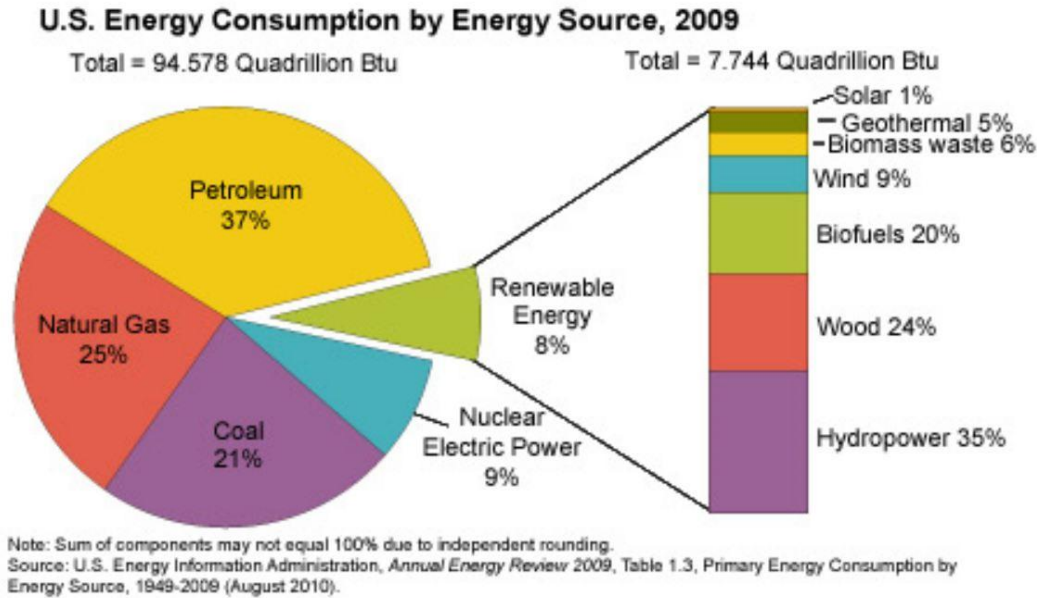
Figure IX-17 Colorado Natural Gas Retail Sales



Renewable Resources

Renewable Energy refers to energy produced from naturally replenishing sources like wind, precipitation, tidal forces, geothermal activity, hydroelectric, and some forms of biomass.

Figure IX-18 U.S. Energy Consumption by Source, 2009

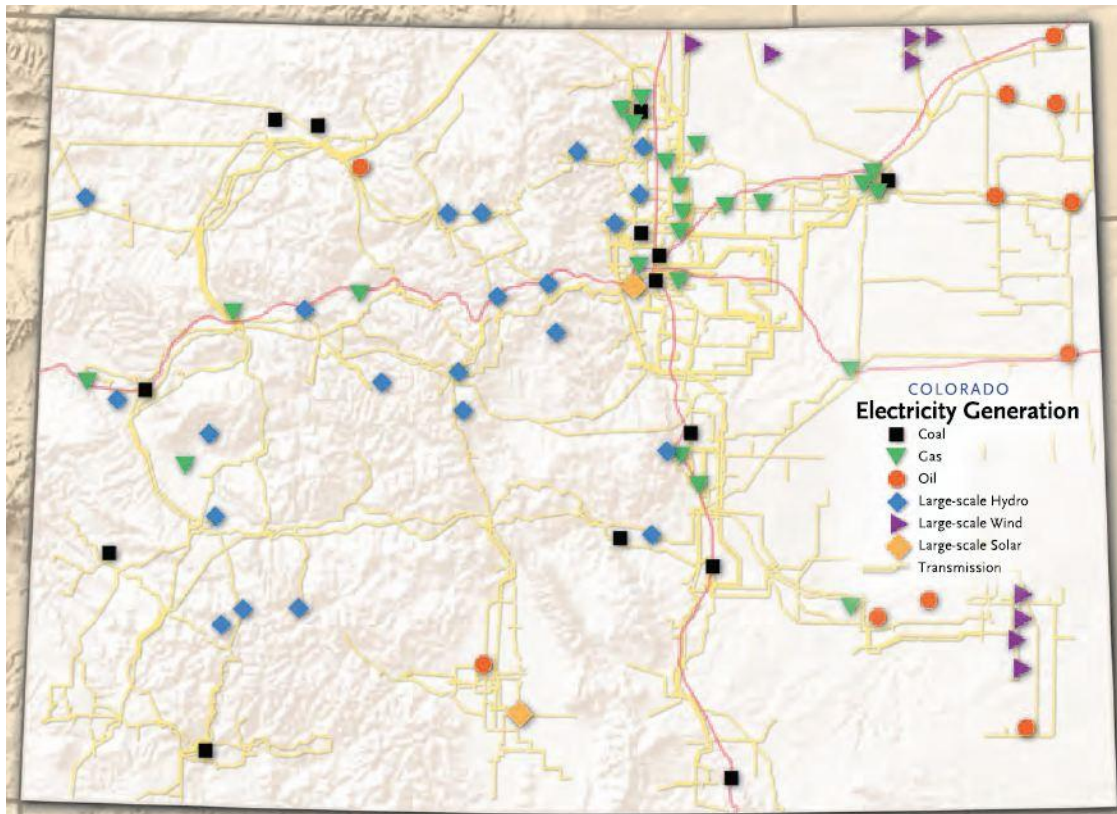


In the United States, most renewable energy sources generate via turbine, and supply the electrical power grid. Renewable energy technologies may have *variable or intermittent output*, meaning that they cannot be optimized as dispatchable energy resource. This introduces challenges to the incorporation of some renewables into grid operations, which must continually adjust to variable load demands. Renewable resources generally require large capital investments but have low operating costs over time. These resources may also require additional investment in transmission or storage to improve reliability.

Costs of renewable development and operation have declined precipitously over recent decades, rendering many renewable generating technologies far more economically viable than in the past. However, the cost of building conversion and transport capacity in the geographically and infra-structurally isolated areas where renewable sources are typically available, and the need to accommodate variable demand with variable generating outputs, are responsible for much of the remaining development challenge. The challenges of conversion and transport can be reduced through smaller scale distributed generation and micro-grid development. Distributed Generation via renewables can contribute to grid operations, either producing power for distribution via a smart grid system, or decreasing demand through local generating capacity. However, Distributed Generation does not benefit from economies of scale to the extent that a more centralized and non-distributed grid model does. The investment in large-scale smart grid

penetration to enhance and encourage distributed renewables generation would also increase the benefits of large-scale renewables.

Figure IX-19 Colorado Electricity Generation Mix



Source: SB-91, Renewable Resource Generation Development Areas Task Force, 2007

Renewable sources currently account for approximately 10% of the US electrical generation, and contribute approximately 8% to the total US energy demand. Roughly 53% of all energy generated by renewables was consumed by electricity producers for generation in 2009, with a significant portion (26%) of total renewable energy usage accounted for by biomass consumption in paper-making and other industrial applications. In the US, the largest portion of renewable-generated electricity originates from hydroelectric generation facilities (66%), followed by wind (17%), wood biomass (9%), waste biomass (4%), geothermal (4%), and solar (0.2%). Overall, the United States is ranked second behind China in total renewable generation, but because China's energy sector profile derives a much higher proportion of its power from hydroelectric than the United States, the United States leads in non-hydroelectric renewable generation.



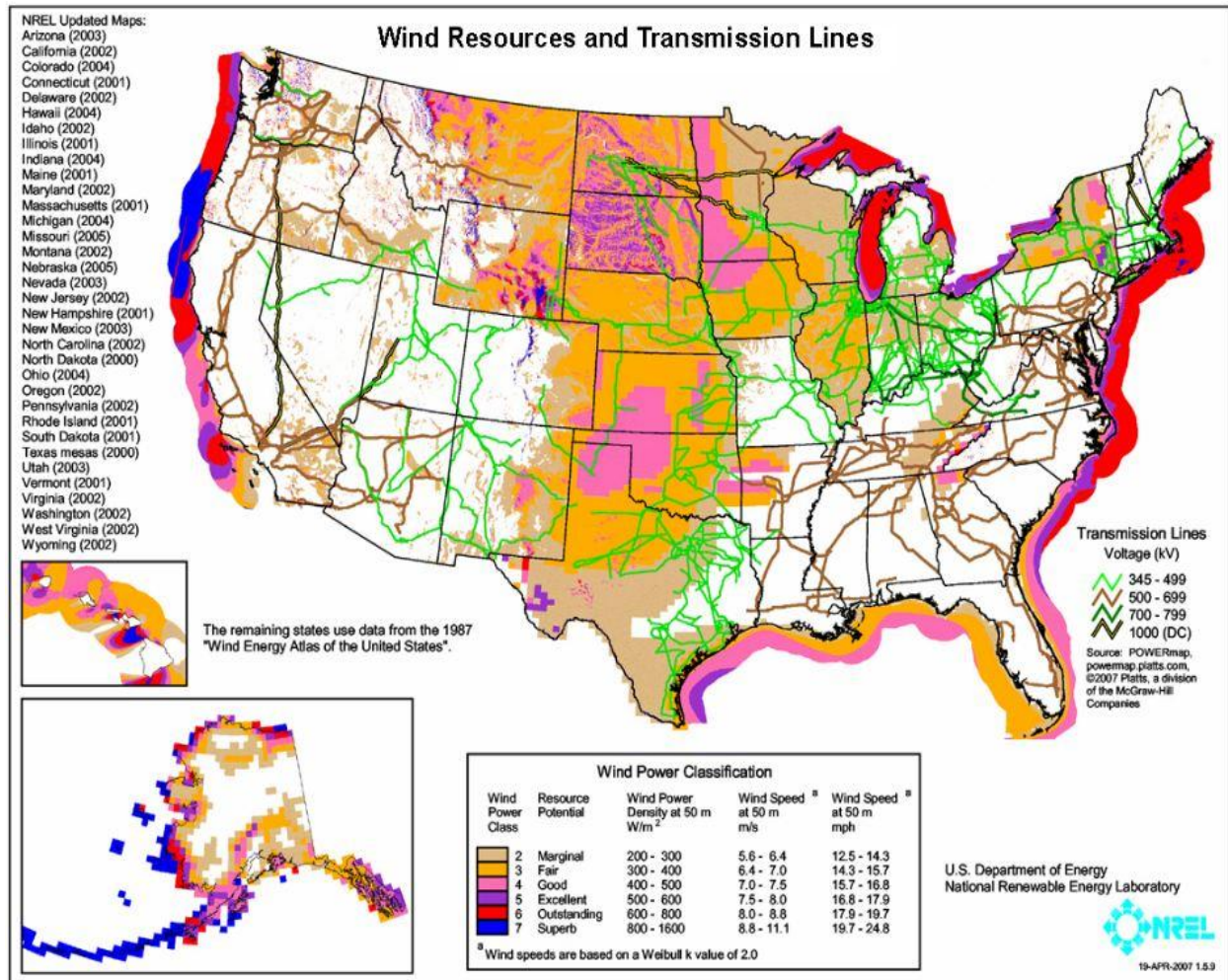
A wind farm near Grover, CO.
(Photo by Carlye Calvin)

Types of Renewable Energy Technologies

Wind

Wind is captured via turbine for electrical generation. Historically, wind has been utilized in many industrial and agricultural applications for mechanical energy only, with no electrical conversion. However, turbine generation is today the primary form of wind power in use, and is the form of wind power with relevance to energy sector operations. While wind turbine generation technologies have been available since the 1920s, research and development from the 1970s forward have resulted in significant increases in the size, reliability, and output of turbine generating systems. Today, turbines capable of generating in excess of 7MW per unit are operational in large arrays across wind corridors in the United States and abroad.

Figure IX-20 Wind Resources and Transmission Lines



This map developed by NREL in 2005, illustrates the high potential for wind development in many US states, including Colorado. However, the map also illustrates that many of the highest-potential wind corridors are located in areas of limited transmission capacity.

Wind energy represents one of the world's largest sources of electrical generation potential. The Max Planck Institute calculates that total extractable wind potential across the globe may range

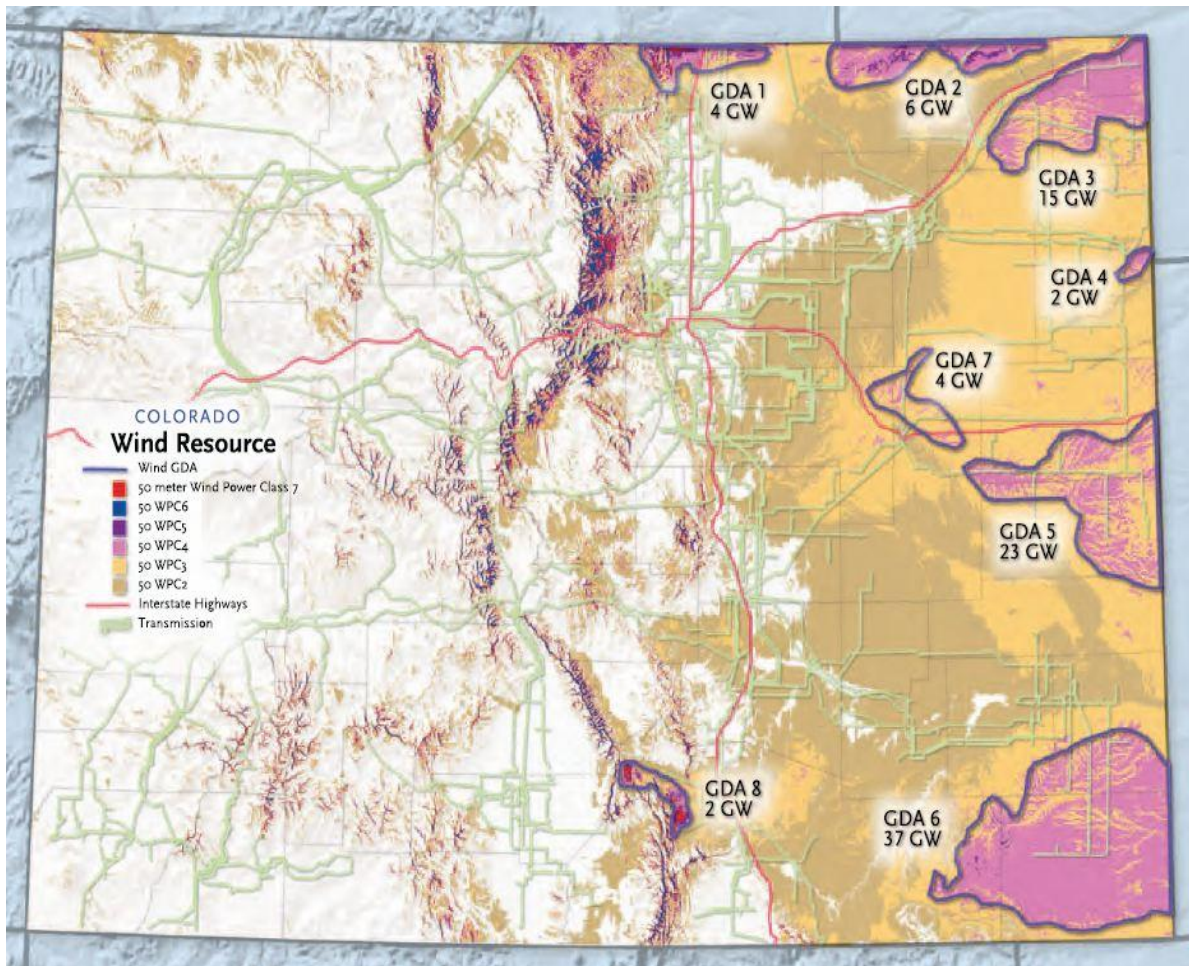
between 18-68TW, considerably outstripping all current global electrical consumption. Other estimates based on measured wind speed assessments have concluded that the total extractable wind energy may range as high as 170TW globally. The cumulative environmental impact of high levels of wind energy extraction are not fully understood, but is unlikely to become significant until a much larger proportion of total global wind potential is tapped.

Wind farms involve multiple turbine generators interconnected to a medium voltage power collection and regulation system, and communications network for monitoring and control. Once the wind's mechanical energy is converted to electrical energy by the collection system, the electrical energy is then converted to higher voltage by a step up transformer substation, and transported along high voltage transmission lines to points of use. Induction generators are often utilized for wind power generation. Combined with variable output, this often requires wind substations to include large capacitor banks for power factor correction, so that wind energy output can remain stable enough to contribute to energy transmission and distribution systems without risk of disruption.

As a rapidly growing section of the US and global energy portfolio, wind production is expected to become more cost-effective over time. Wind development is the most rapidly-growing segment of renewable electric generation in most countries, including the United States.

Wind Generation in Colorado: In Colorado, significant wind corridors and potential development zones are concentrated primarily in the Front Range foothills and eastern plains, and potential for future wind development is strong. The eight identified wind GDAs have development potential of over 96 GW of capacity, over eight times Colorado's current use. As of 2011, an estimated 9.2% of Colorado's total electric generation portfolio is sourced from wind generation, ranking Colorado 6th in the US when measuring wind as a percentage of total generating output. Given the generation potential of Colorado's wind resources, there is interest in developing wind export capacity to other states in the Southwestern region.

Figure IX-21 Wind Generation Development Areas



Source: SB-91, Renewable Resource Generation Development Areas Task Force, 2007

In Colorado as with many western states, the primary challenge to increased wind development is not a lack of wind resources, but the need to expand and update transmission capacities to accommodate the inputs from new wind developments.

Solar

Solar energy can be captured by solar thermal energy systems, which capture solar heat, and photovoltaic systems, which capture solar light and convert immediately to direct current. Both forms of solar energy generation combined represent only 1-2% of total renewable electric generation worldwide, but are developing rapidly. There are challenges associated with solar development, and all solar generation is variable output. However, as with wind, the untapped energy potential of sunlight is thousands of times greater than global energy demand.

Solar thermal energy is classified as low, medium, or high-temperature. Low and medium temperature collection systems are increasingly utilized to support heating and water systems in home and business applications, but do not typically generate electrical power. Larger scale high temperature thermal collectors may be utilized for electrical generation.

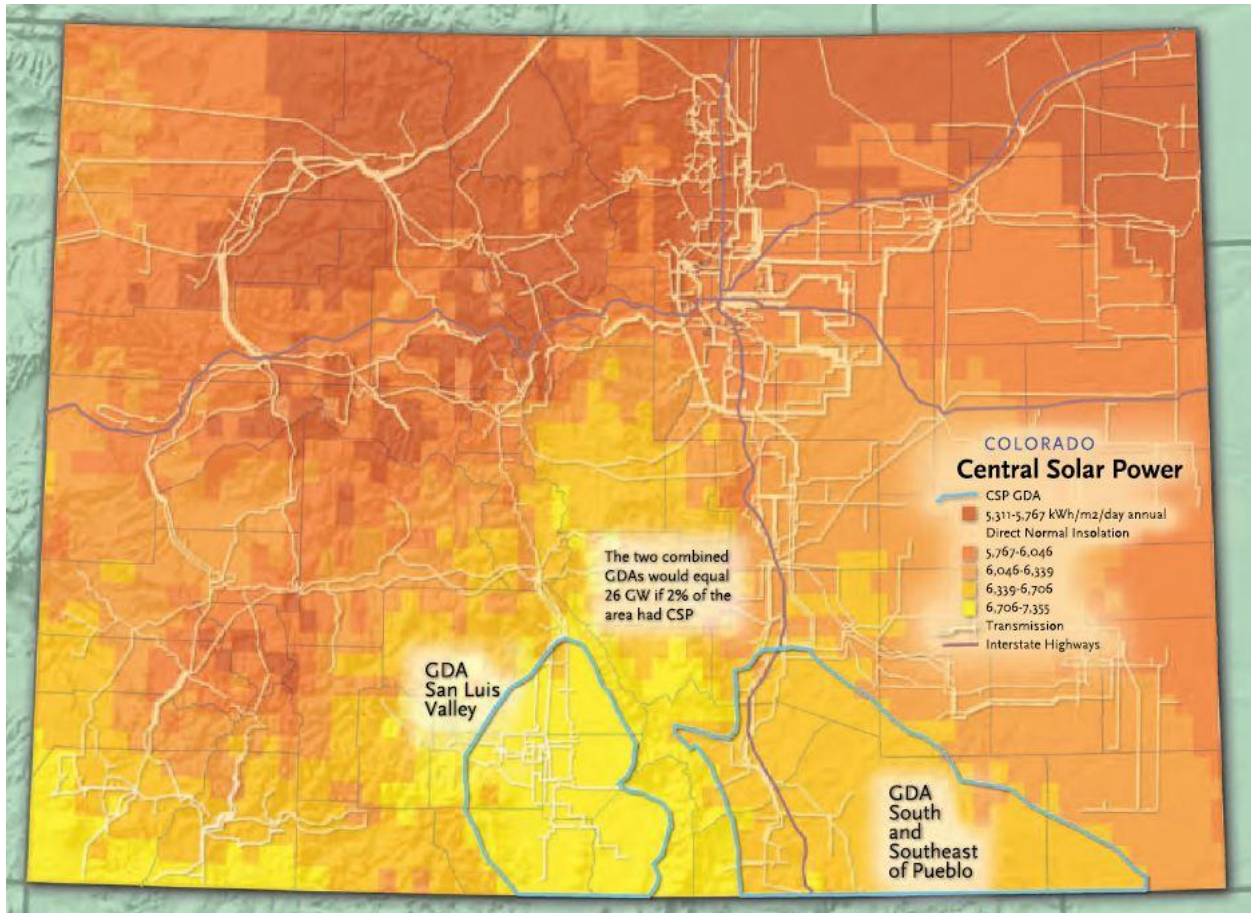
Micro-generation utilizing PV is a rapidly growing industry. Development of solar bulk generation has been slow relative to other renewables due to high initial capital investment costs, and lack of transmission capacity from solar fields. However, development costs per KW are decreasing, and larger scale solar development is underway in many US states and across the globe.

Colorado Solar Generation: Solar micro-generation is quickly developing in many business, government, and residential applications. PV generation including both bulk and distributed generation grew from 4MW in 2006, to 103MW in 2010. Zones identified for high development potential include the San Luis Valley and areas southeast of Pueblo. Colorado's solar generating potential within the identified GDA corridors can hypothetically produce 1300GW. NREL calculates that if 2% of developable solar resource areas were utilized, generating potential of 26GW could be developed.



Solar Thermal Collector System
 Thermal collectors capture solar energy and convert to heat, which is then utilized directly, or converted to electricity. Pictured: A medium temperature parabolic trough solar thermal collector system provides for facility and water heating at Jefferson County Detention Center in Golden, CO. Image: NREL, 2011

Figure IX-22 Colorado Central Solar Power



Source: SB-91, Renewable Resource Generation Development Areas Task Force, 2007

Geothermal

Geothermal energy is heat energy stored in the Earth. Geothermal energy can be captured for direct application, which makes direct use of captured heat, and for bulk electrical generation, which typically converts heat to electrical power via turbine. Geothermal generation is reliable, and because it requires no fuels to operate, it is largely immune to cost fluctuations or supply shortages. Approximately 10,715MW is generated globally by geothermal, from facilities in 24 countries. Another 28 GW of direct application geothermal heating is produced annually across the globe. Development of

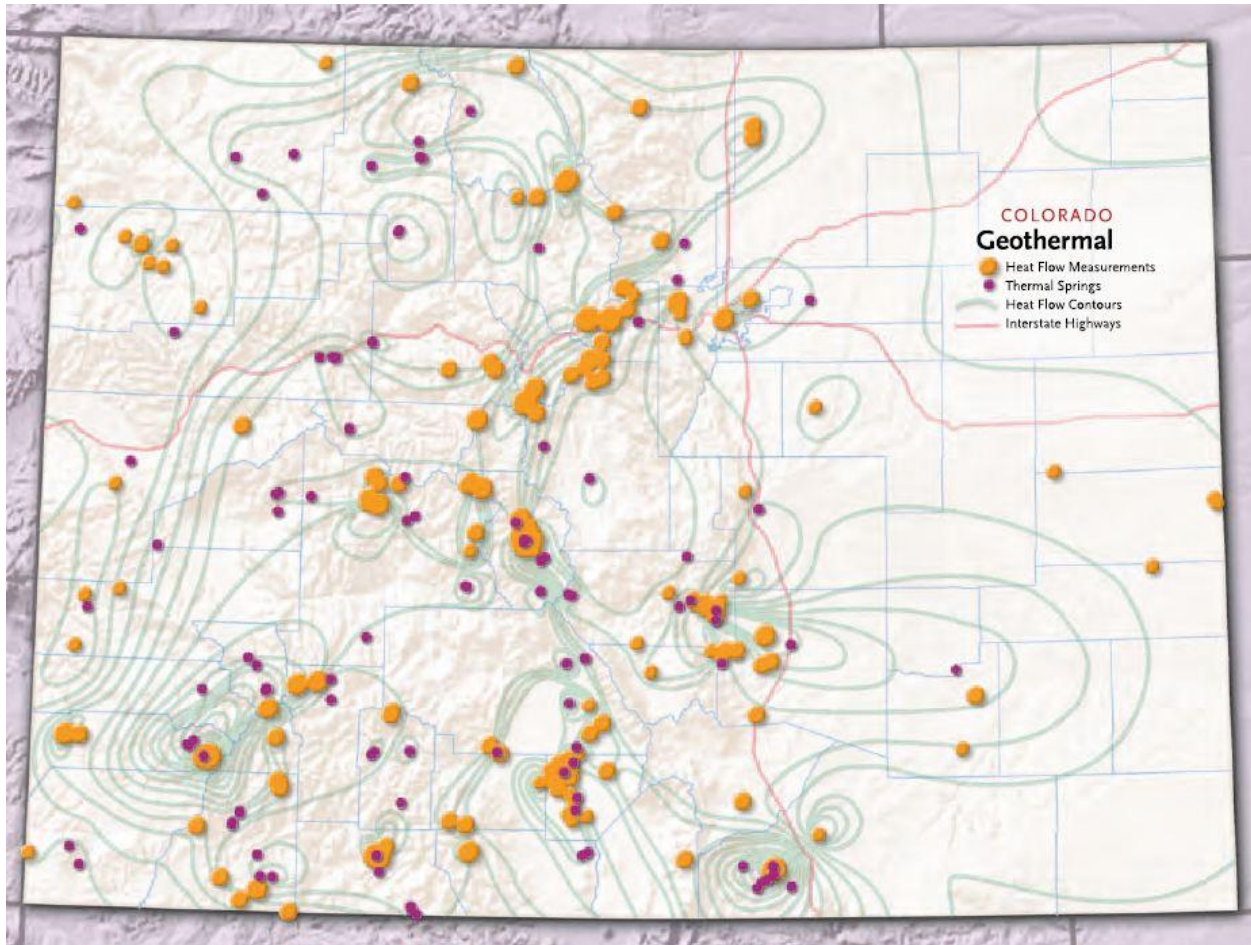


Iceland Geothermal Plant

Economies with relatively low electrical demand and relatively high supply of available geothermal resources can derive substantial portions of their electric power mix from this reliable and environmentally-friendly source. Pictured: A geothermal generating plant in Iceland. Iceland derives 30% of its total electrical energy from geothermal sources.

geothermal generating capacity has been rapid in recent years, but geothermal generating capability is limited to areas where geothermal heat is available, often near faults or in seismically active zones.

Figure IX-23 Geothermal Heat Flow Measurements and Thermal Springs



Source: SB07-091 Renewable Resource Generation Development Areas Task Force

As with solar and wind, unexploited geothermal resources are estimated to far exceed total global energy demand, however, drilling for deep geothermal resources can be risky, and is often capital intensive. In addition, only a fraction of total geothermal potential can be reached with current drilling and generating methods. The United States leads the world in total geothermal generating capacity, but geothermal accounts for only 0.3% of national electrical production. Some US states with significant geothermal resources, have incorporated geothermal generation as a significant portion of their power mix. California derives 5% of its power mix from geothermal, and Nevada is planning to derive nearly 25% of its electrical power from geothermal within the next ten years.

Geothermal in Colorado: Colorado has access to some of the best geothermal resources in the US, ranking 4th in the nation for accessible geothermal resources capable of driving electrical production.

Biomass/Biofuels

Biomass refers to energy derived from biological organisms, and biofuels are fuels whose energy is derived from biological products. Biomass electrical generation is typically produced through burning or gasification of plant or waste matter, and conversion to electricity via turbine or biochemical processes. Biomass burning is a renewable energy source, but unlike other renewables biomass burning is not a zero-emission technology.

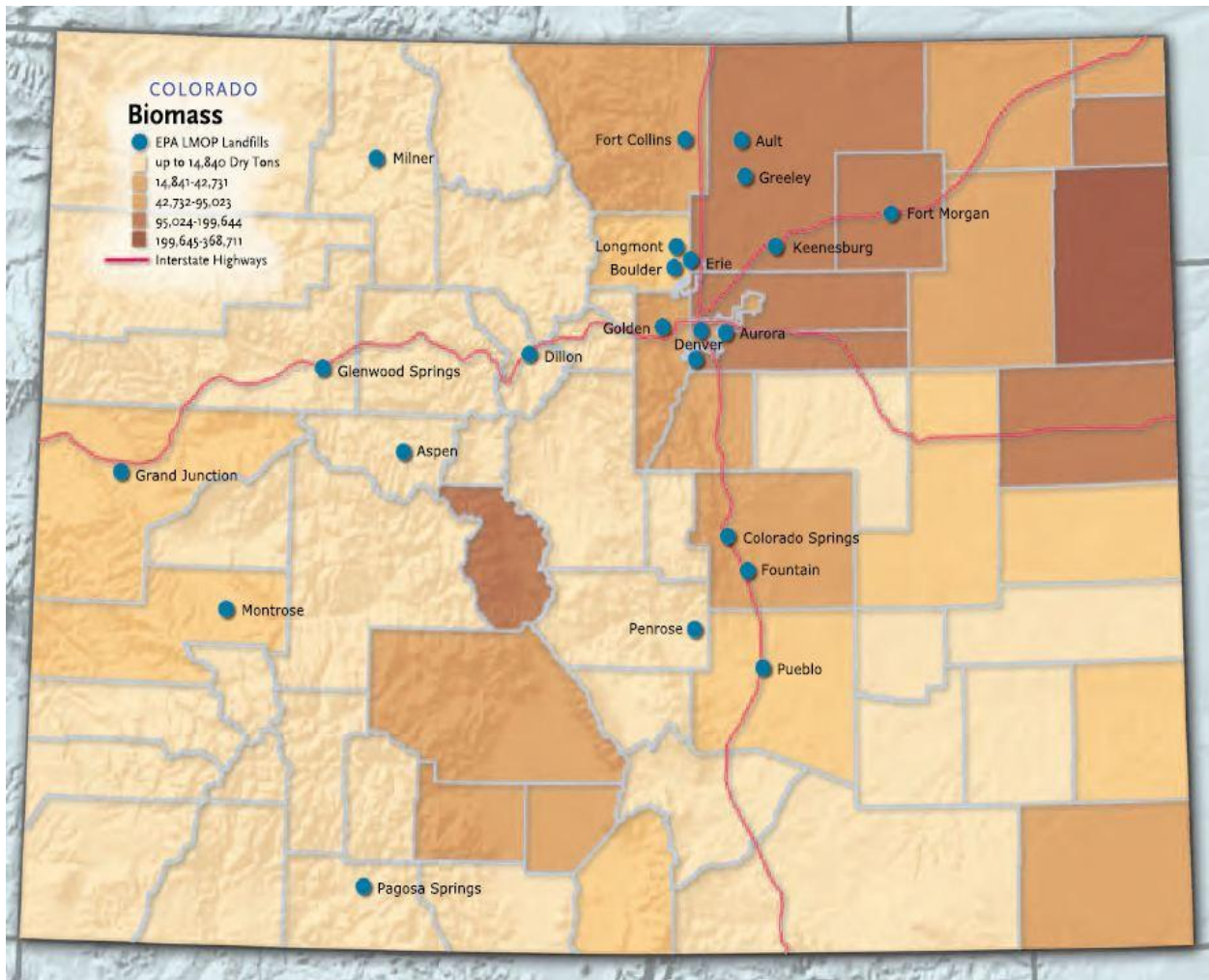
Even as biomass burning emits carbon, it is often utilized to convert forest refuse, dead timber from insect mitigation, or logging byproducts into sustainable energy and *biochar* (a high-performance fertilizer and soil additive which increases plant growth and can be used to offset biomass carbon emissions). Biochemical conversion can also emit biomethane, a potent greenhouse gas if released into the atmosphere, but also a valuable refined fuel. Most electrical generation via biomass burning utilizes plant materials from switchgrass, hemp, corn, sorghum, sugarcane, or oil palm, or burns forest residues and municipal solid waste. Because fuels for biomass generation are bulky and expensive to transport, biomass generating facilities are often located near fuel sources. Private burning of wood biomass is common in both the developed and developing worlds, but biomass electrical generation does not constitute a large portion of global generation capacity. In the United States, biomass generating capacity for a grid operation is approximately 11,000MW, accounting for roughly 1.4% of US electricity supply.

Biofuels are liquid fuels derived from biological products, rather than fossil material. Bioethanol is derived from a variety of plants including corn, beets, sugarcane, and switchgrass. Ethanol is primarily used as a gasoline additive, and the United States and Brazil are leading producers, together accounting for over 90% of global bioethanol production. Biodiesel is derived from vegetable oils and animal fats, and can be used without dilution, or used as a diesel additive. Production of biofuels has increased rapidly in the United States and abroad, and development is expected to continue. The International Energy Agency estimates that emerging biofuels technologies may meet more than 25% of global liquid fuels demand by 2050.

Like petroleum fuels, biofuels must be refined for use as liquid fuel. Unlike petroleum fuels, biofuels materials are not efficiently transportable via pipeline, and are produced in a more dispersed agricultural system, rather than the more centralized petroleum production system. As a result, biofuels currently produce lower average return on investment than petroleum products for conversion to liquid fuels, but improvements to refining methods and refining capacities are expected to further increase economic viability of biofuels considerably over time. Likewise, the precursor materials utilized for biofuels production may vary in energy potential. Biofuels are not zero emission, and are typically energy intensive to produce, but can be lower-emission than comparable petroleum-based liquid fuels, and unlike fossil fuels, are naturally sustainable fuel sources.

Biomass/Biofuels in Colorado: Colorado has a number of operating or planned combustion and biochemical biomass plants, which vary in scale from small-scale combustion units to provide heat and hot water to facilities, to facilities capable of bulk electrical generation.

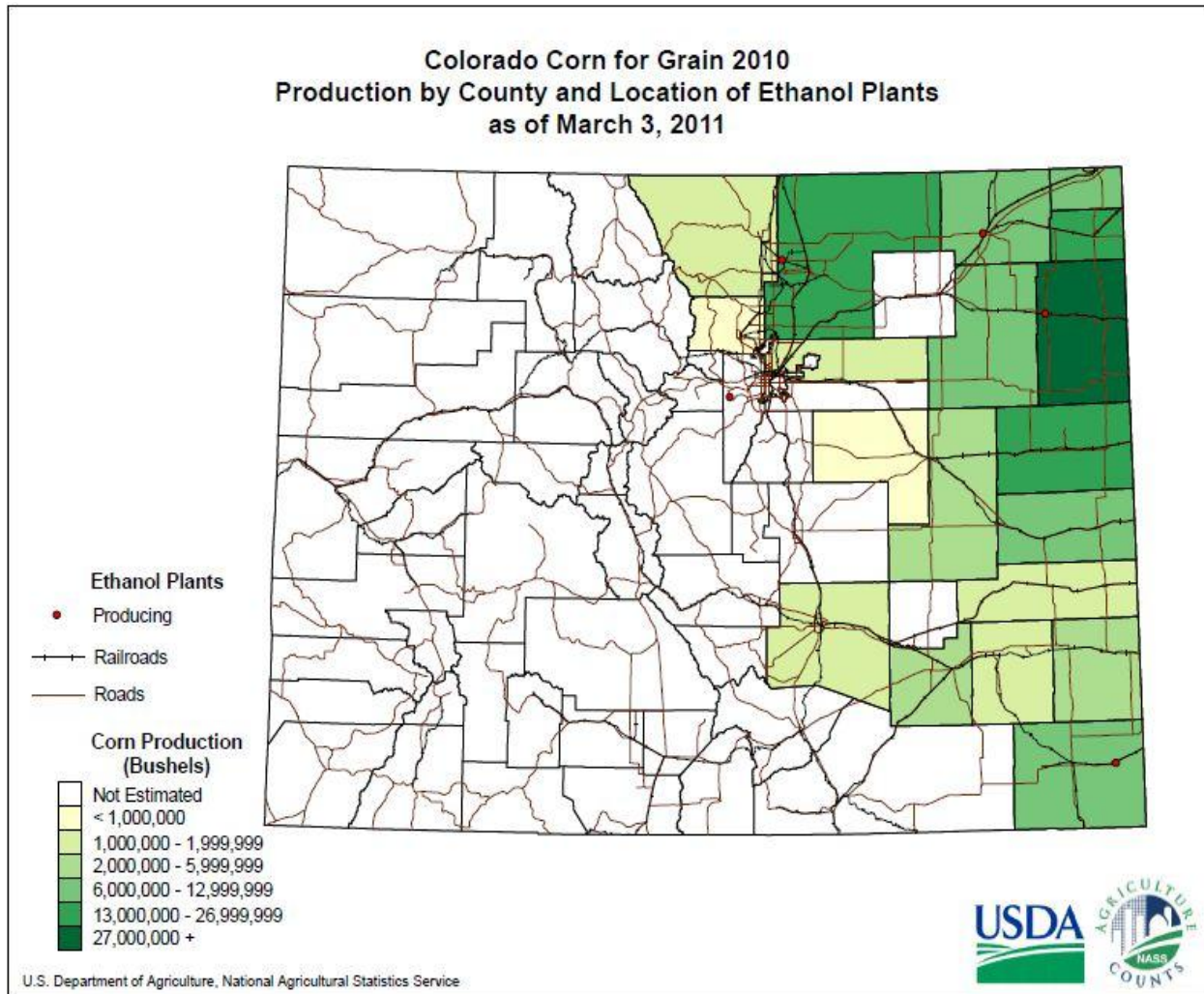
Figure IX-24 Colorado Biomass Plants



Source: SB-91, Renewable Resource Generation Development Areas Task Force, 2007

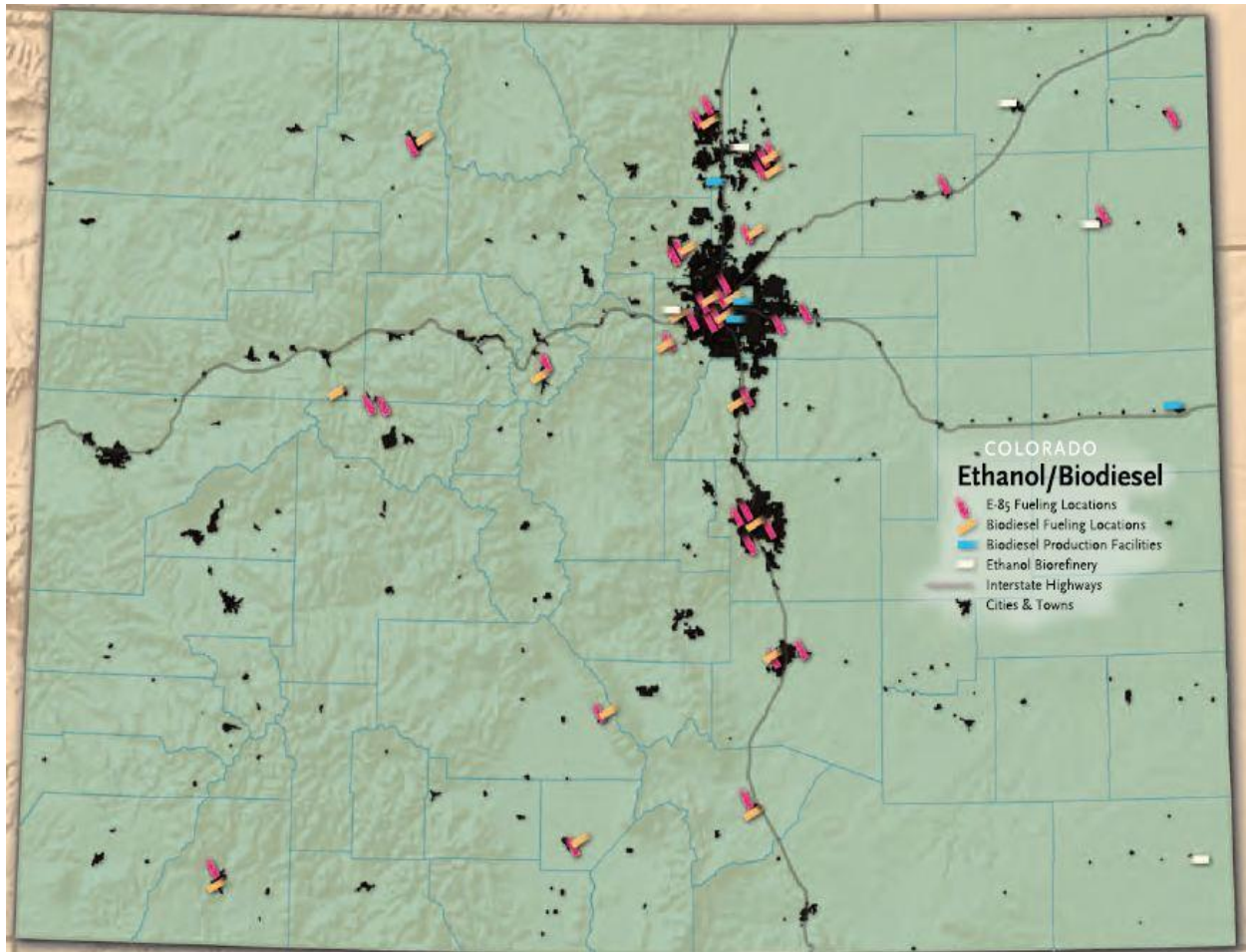
Biofuels production capacity has grown in recent years, but growth may be impacted by the availability and price of corn imports from out of state. Figure IX-25 below indicates the Colorado corn production in 2010 for Ethanol.

Figure IX-25 Colorado Corn Production for Ethanol



Colorado also has several biodiesel and bioethanol refineries, primarily located near the Denver Metro area and in eastern portions of the state.

Figure IX-26 Colorado Ethanol/Biodiesel



Source: SB-91, Renewable Resource Generation Development Areas Task Force, 2007

Coal

Coal is a very dense sedimentary rock formed from the remains of trees, ferns, and other ancient plant materials exposed to intense heat and pressure over hundreds of millions of years. The first coal mine in Colorado was constructed during the Pike’s Peak Gold Rush in 1859 near Marshall Mesa and the city of Boulder. Over 150 years later, more than half of Colorado’s electricity is generated at coal-fired power plants.

By 2011, Colorado was ranked 9th in total US coal production. Additionally, within the state of Colorado coal represents the majority of energy generation at 57%. Through the Clean Air Clean Jobs Act¹, Xcel Energy has agreed to retire approximately 600 megawatts of coal generation, switch about 450 megawatts of coal to natural gas, add 570 megawatts of new natural resource generation, and install modern emission controls on 950 megawatts of existing coal generation.

¹ http://rechargecolorado.org/images/uploads/pdfs/Colorado_Clean_Air_Clean_Jobs_Act_GEO_WhitePaper.pdf


Different utilities use a different mix of resources for electricity generation. Investor owned utilities, like Xcel Energy and Black Hills Energy, who service the largest population of energy consumers in Colorado, use coal to produce 52.3% of their electricity. However, investor owned utilities use a lower proportion of coal than municipal utilities or rural electric cooperatives. Municipal utilities, for example, use 14% more coal for electricity production than IOU’s.

Table IX-5 Colorado Electric Resource Mix for Colorado Utilities

Utility Type	Coal	Natural Gas	Hydroelectric	Non-Hydro Renewable	Other
Investor Owned Utilities	52.3%	35.4%	1.9%	9.7%	0.7%
Rural Electric Cooperatives	62.6%	11.2%	9.3%	3.3%	13.6%
Municipal Utilities	66.5%	18.2%	11.7%	2.1%	1.6%

Source: 2010 Colorado Utilities Report

Coal Types



Type of Coal	Carbon Content	BTU/ton
Bituminous	60-80%	21-30 million
Sub-Bituminous	34-45%	16-24 million
Anthracite	80-96%	20-28 million

Source: Colorado Geological Survey

Colorado extracts coal from both surface mines and underground mines; most of which are located in the western portion of the state. Bituminous Coal is the most common type of coal found in the United States and the majority of coal found in Colorado is classified as Medium/High Volatile Bituminous or Sub-Bituminous. Sub-bituminous coal accounts for 47% of the coal produced in the United States. Demand for Colorado coal is high and the state currently exports coal to twenty-four additional states, the country of Mexico, and many countries in Europe.

Physical Facilities and Systems

Surface and Underground Mines:

Surface mines recover greater proportions of the coal deposit than underground mines. There are four techniques used to extract coal from surface mines: area mining, contour mining, mountaintop removal, and room and pillar mining. Globally, about 40% of coal production involves surface mining.

The remaining 60% of coal resides too deep underground to extract from the surface. There are five methods for underground mining and these are generally determined by the type of equipment used to extract the coal: longwall mining (longwall shearer), continuous mining (Continuous Miner Machine), blast mining (explosives), shortwall mining (<1% of underground mining), and retreat mining (the most dangerous method, as the pillars holding up the mine roof are collapsed to expose additional coal).

Both underground and surface mining techniques represent a disaster risk for humans and the surrounding environment. Underground mining is the most dangerous technique with the “Fall of Ground” accounting for 35% of fatalities, “Powered Haulage” (vertical transportation of humans, coal, equipment or waste) at 30.2%, and “Ignition of Gas/Dust” at 18%.

Surface mining accidents typically involve machinery, rock fall, and electrical shock.

Coal Handling and Preparation Plant (CHPP):

Coal preparation and processing plants break, crush, screen, clean and/or use heat to fry coal at mines, power plants, cement plants, coke manufacturing facilities and industrial facilities. Coal preparation increases the heating value of coal by removing impurities and lowers the cost of transporting coal (up to 60% of raw coal may be contaminated with impurities, rock, dust etc.).

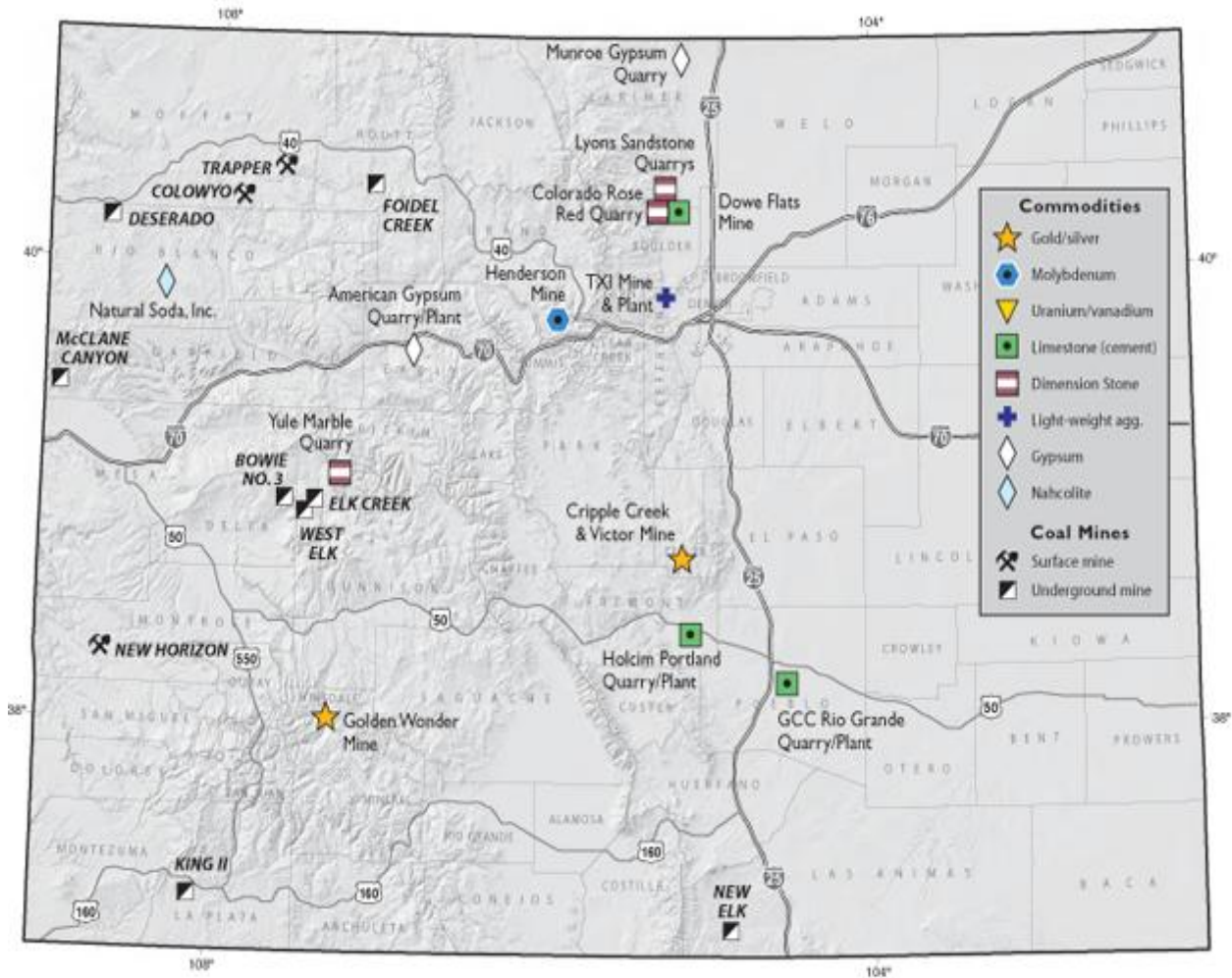
Coal Slurry Storage and Impoundment:

Coal slurry is a liquid and/or solid by-product of coal preparation and processing. This material is either stored in above-ground man-made reservoirs or injected back into abandoned mines.

Top Ten Power Plants in Colorado	
Generating Capacity	
1)	Comanche- 1,427 MW Public Service Company of Colorado Coal
2)	Craig- 1,311 MW Tri-State Generation and Transmission Coal
3)	Fort St. Vrain- 969 MW Public Service Company of Colorado Gas
4)	Cherokee- 611 MW Public Service Company of Colorado Coal
5)	Rawhide- Coal 280 MW, Gas 388 MW Platte River Power Authority Coal & Natural Gas
6)	Rocky Mountain Energy Center- 601 MW Rocky Mountain Energy Center Gas
7)	Pawnee- 505 MW Public Service Company of Colorado Coal
8)	Front Range Power Project- 480 MW City of Colorado Springs Gas
9)	Hayden- 446 MW Public Service Company of Colorado Coal
10)	Cabin Creek- 324 MW Public Service Company of Colorado Hydroelectric Pumped Storage

Coal Extraction and Production in Colorado

Figure IX-27 Mines in Colorado



Source: Colorado Mining Association

Colorado is home to ten coal mines in eight western counties. Seven of these mines are underground (five are Longwall mines) and three are surface mines. In 2008, Colorado coal mines extracted approximately 32 million tons of coal with a production value of \$887 million. Nearly 40% of the coal extracted from the state of Colorado is distributed to power plants throughout the state, while the remaining 60% is exported to other states by rail.

Seven of the ten largest power plants in Colorado are fueled by coal; the Comanche coal power plant south of Pueblo is the largest net producer of electricity in the state of Colorado.

Table IX-6 Colorado Coal Mines

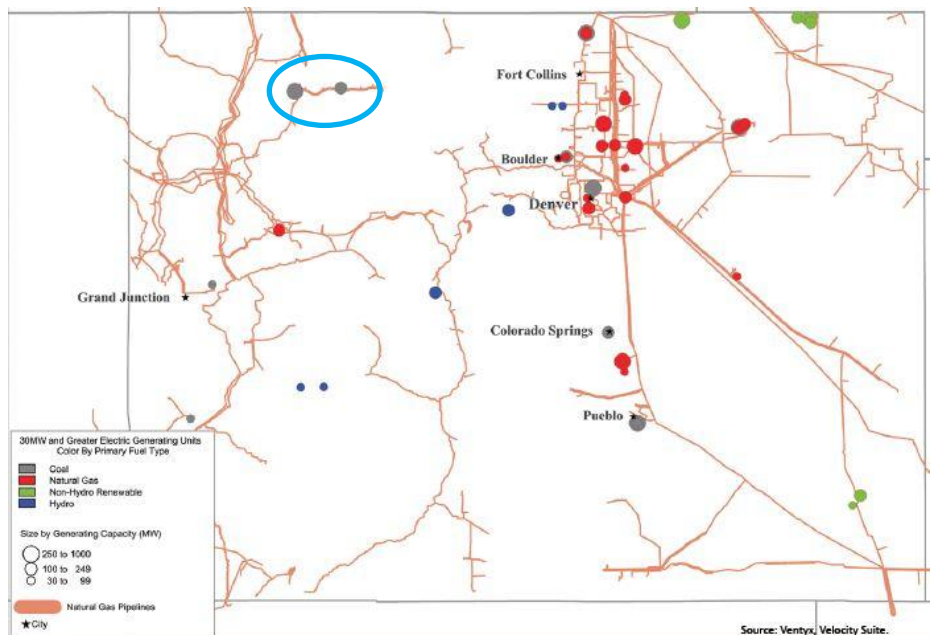
Coal Mines in Colorado 2009/2010 County and Mine Type (thousand short tons)						
County	Underground Mines		Surface Mines		Total Mines	
	# of Mines	Production	# of Mines	Production	# of Mines	Production
Delta	1	1,325	0	0	1	1,325
Garfield	1	200	0	0	1	200
Gunnison	2	8,588	0	0	2	8,588
La Plata	1	522	0	0	1	522
Moffat	0	0	2	4,785	2	4,785
Montrose	0	0	1	293	1	293
Rio Blanco	1	1,723	0	0	1	1,723
Routt	1	7,727	0	0	1	7,727
Total	7	20,085	3	5,078	10	25,163

Data from the U.S. Energy Information Association, Form EIA-860, "Annual Electric Generator Report"

Coal Transportation

After coal is extracted it is cleaned and processed (often at a CHPP facility close to the mine) and prepared for transport. Railroads move over 70% of the domestic coal in the United States, while trucks account for 11.7 percent, river 11.2 percent and tramway, conveyor, and slurry pipeline at 6.6 percent. In the state of Colorado, 60% of coal is transported by rail to states like Kentucky, Alabama, Texas, Utah, and Wisconsin.

Figure IX-28 Craig and Hayden Power Plants



A large coal train or “unit train” may be over a mile long and carry up to 100 short tons of coal in each train car. To reduce transportation costs, coal-fired power plants are occasionally located

near large coal mines. The Trapper mine is located directly next to the Craig power plant and produces coal exclusively for that facility. Additionally, the Colowyo, Deserado, and Foidel coal mines in northwest Colorado are located close to two of the state’s largest coal-fired power plants: the Craig Power Plant owned by Tri-State Generation and Transmission and the Hayden Power Plant owned by Xcel Energy.

Within the state of Colorado, coal is transported by both rail and truck. In 2010, 5,788 thousand short tons of coal were shipped by train and 4,286 thousand short tons by truck. The following table shows the distribution and transportation mode of coal within the state of Colorado and to the states of Kentucky and Alabama (the two largest Colorado coal importers).

Table IX-7 Coal Distribution and Transportation Mode

Coal Distribution & Transportation Mode by the State of Colorado, 2010 (thousand short tons)					
Destination State	Transportation Mode	Electricity Generation	Industrial Plants	Commercial and Industrial Customers	Total
Colorado	Total	9500	310	265	10074
	Railroad	5226	310	252	5788
	Truck	4274		12	4286
Kentucky	Total	2123	-	-	2123
	Railroad	2123	-	-	2123
Alabama	Total	2113	-	-	2113
	Railroad	2113	-	-	2113

Source: EIA Annual Coal Distribution Report

Hydroelectric

Hydroelectric plants produce about seven percent of the total electricity in the United States. Currently, hydropower facilities in the United States can generate enough hydroelectricity to power 28 million households.

Table IX-8 Hydroelectric Net Generation (by State)

Net Generation from Hydroelectric Power by State and Sector 2009/2010						
State	Electric Utilities (MW)		Independent Power Producers (MW)		Total (MW)	
	2009	2010	2009	2010	2009	2010
Colorado	1727	1589	159 MW	157	1886	1746
Idaho	9691	8443	744	718	10434	9161
Montana	5890	5811	3616	3419	9506	9230
New Mexico	271	253	-	-	271	253
Utah	827	784	-	8	835	792
Wyoming	967	1018	-	-	967	1018

Source: US Energy Information Administration (EIA)

In Colorado, the annual net hydroelectricity generation averages about 1.6 million megawatt hours, which comprises only 0.3 percent of total hydroelectricity generation in the United States. Major rivers flowing from the Rocky Mountains offer hydroelectric power resources. Since 2001, net hydroelectricity generation has been declining, most likely due to reduced stream flows

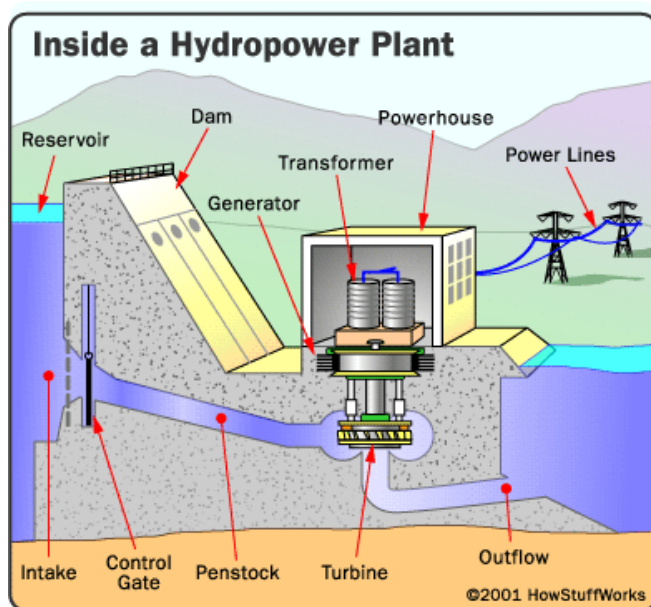
and low water levels in reservoirs around the state. Additionally, seasonal recreation variation may place restraints on hydroelectric production.

According to a 2005 inventory by the NREL, there are sixty-two operating hydropower facilities in Colorado. These facilities range in size from 5 KW to 300 MW. Three of these facilities are pumped storage, with the largest being the Cabin Creek Generating Station near Georgetown, Colorado.

Physical Facilities and Systems

Dam: Most hydroelectric power plants rely on a physical barrier to store water in large reservoirs. In Colorado there are approximately 1,900 dams; with some storing water for consumption and others for electric power generation.

Figure IX-29 Hydropower Plant

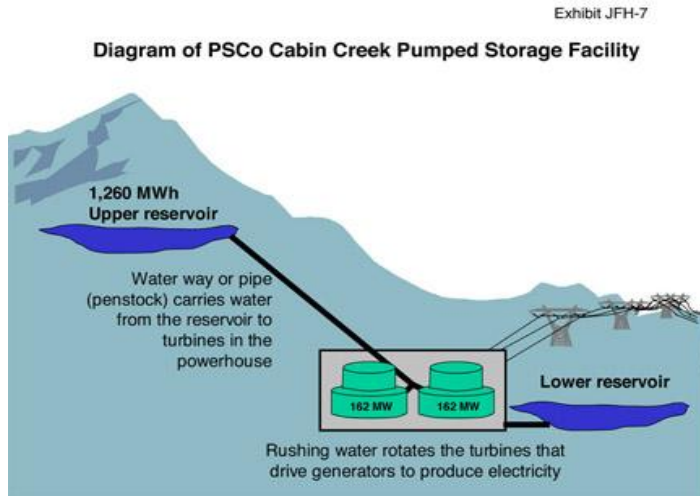


Turbine & Generator: Gravity causes water to flow through the dam's intake, down through the penstock, and on to the turbine. The water then strikes the blades of the turbine causing it to turn. This movement causes a series of magnets within the generator to rotate past copper coils and produce alternating current (AC). The transformer then converts the electricity to a higher-voltage current.

Pumped Storage Plant: Pumped storage hydroelectric plants are facilities with upper and lower reservoirs designed to store varying levels of water to accommodate high demand at peak seasons. During normal operations, pumped storage plants operate at a lower output; excess water is pumped and stored in the higher reservoir until it is needed. Colorado has three of these plants. Variable output facilities like these reduce the need for new generating plants and permit

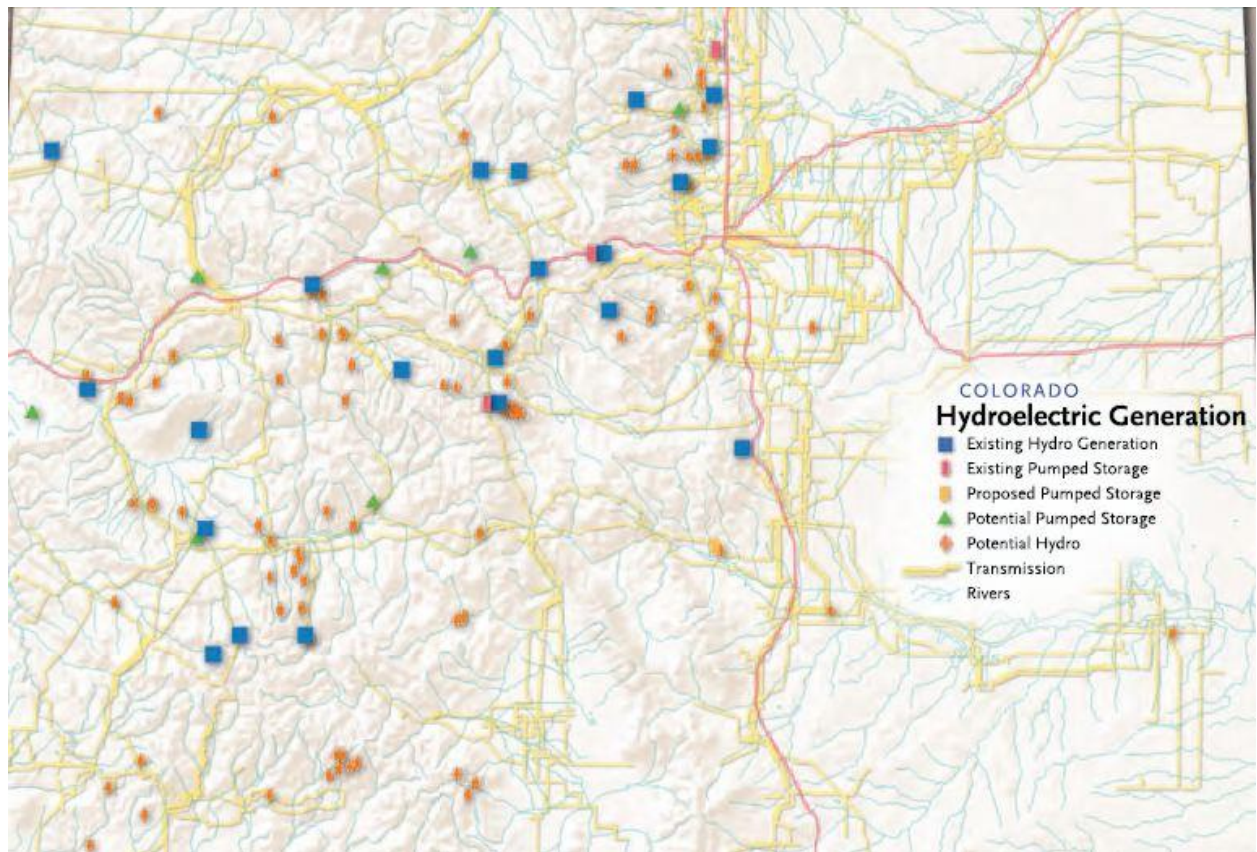
existing power plants to operate at their most efficient capacity. The state of Colorado is well suited to use pumped storage plants with its high mountains and major rivers.

Figure IX-30 Pumped Storage Facility



Existing and Potential Hydroelectric Generation Sites in Colorado

Figure IX-31 Colorado Hydroelectric Generation



Source: SB-91, Renewable Resource Generation Development Areas Task Force, 2007

Liquid Fuels

Liquid fuels comprise the largest source of energy consumption in the United States at a consumption rate of 41 quadrillion Btu’s per year. It is projected that the domestic supply of liquid fuels will grow as a result of domestic oil production, an increase in the use of biofuels, and slower growth in the consumption of transportation fuels. Consequently, the United State’s dependence on imported



The Suncor Refinery in Commerce City, CO

liquid fuels is predicted to decline. Liquid fuels are an integral part of a state’s economy including both distribution and delivery. The quality of life for Colorado’s citizens and the sustainability of critical services depends on the vitality of liquid fuels power delivery.

In 2009, Colorado consumed 79.5 million barrels of oil (or their equivalents) for transportation purposes- over 3 billion gallons or 218,000 barrels per day (bpd). The breakdown of fuel types is shown in Table IX-9 and Figure IX-32 below².

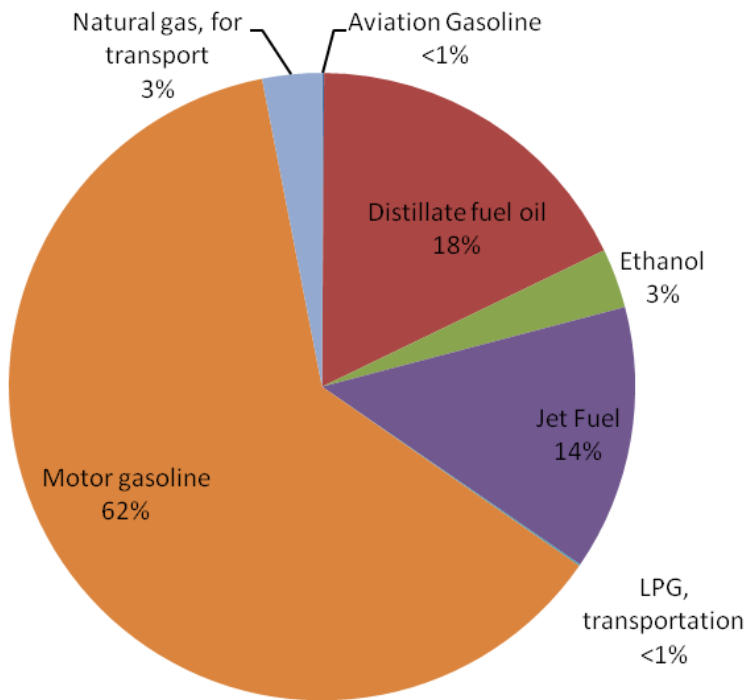
Table IX-9 Colorado Usage of Fuels in Transportation in 2009 (by product)

Fuel	Motor Gasoline	Distillate Fuel Oil (Diesel)	Jet Fuel	Ethanol	Natural Gas	LPG (propane)	Lubricants	Aviation Gasoline	Total
Consumption (thousand barrels)	49,364	14,064	10,842	2433	2437	66	298	83	79,587
Consumption per day (thousand barrels)	135.2	38.5	29.7	6.67	6.67	0.18	0.82	0.23	218.0

Source: Energy Information Administration

² http://www.eia.gov/state/seds/hf.jsp?incfile=sep_use/tra/use_tra_CO.html&mstate=Colorado

Figure IX-32 Colorado Consumption of Transportation Fuels



Source: Energy Information Administration 2009 data.

Fifty percent (50%) of the crude supply originates from Canada and states north of Colorado. Approximately 16% of Colorado’s liquid fuels are extracted, refined, and marketed in Colorado. Suncor supplies around 34% of the gasoline and 54% of the diesel that is consumed in Colorado.

Colorado has two Suncor refineries in Commerce City that process approximately 100,000 barrels of crude oil per day. In addition, Colorado Fuels Manufacturers (CFM) has a fractionation and blending facility in Fruita, Colorado where it refines about 2,000 barrels of local (100 mi radius) crude daily and produces raw gasoline, propane and butane.

There are numerous statewide and regional distributors providing bulk storage, delivery, and wholesale operations. Wholesale fuels are transported by truck to approximately 2,800

Just In Time Delivery

Just in Time or JIT delivery is a production strategy used by liquid fuel distributors and other manufacturers to minimize inventory carrying costs by distributing the product only when it is needed. Proponents of JIT production believe that “inventory is waste” and that fuel delivery is more efficient when it is transported directly to trucks and pipelines rather than large storage tanks for usage later.

Benefits:

- Minimizes storage requirements, inventory costs, and carrying costs

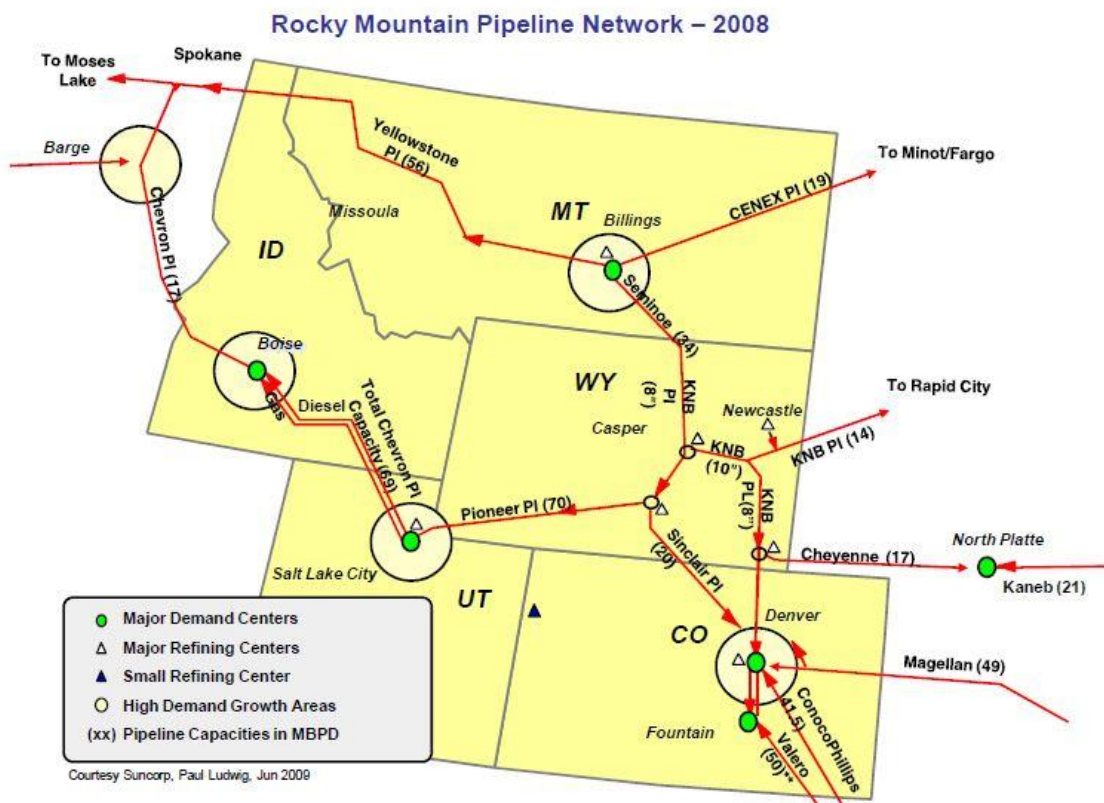
Drawbacks

- Smaller stores of finished fuels may introduce new vulnerabilities into regional fuel prices.
- Supply-side shocks may have a more significant impact on down-stream distributors and consumers

retail vendors (in 2009). The average retailer has storage capacity of about 20-30,000 gallons while larger retailers may store up to 60,000 gallons. Colorado’s 75 airports receive around 1.3 million gallons of jet fuel and 65,000 gallons of aviation gas each day. Due to market volatility and “just in time” inventory practices, fuel stockpiles are generally limited and are estimated to provide about five days of reserves.

The majority of Colorado’s liquid fuels are imported via five pipelines of the Rocky Mountain Pipeline Network. These pipelines terminate at various fuel rack locations along the Front Range. Colorado’s position at “the end of the pipeline” makes it more vulnerable to supply disruptions. However, this vulnerability is partially mitigated by local crude extraction and refinery operations.

Figure IX-33 Rocky Mountain Pipeline Network



Colorado lies at the intersection of five major liquid fuel pipelines: Valero, ConocoPhillips, Magellan, KNB, and Sinclair

Colorado oil production amounts to approximately 1% of total US crude oil production. Although this accounts for a very small percentage of oil production in the United States, the state is also home to enormous deposits of oil shale rock (marlstone) which can be converted into crude oil through destructive distillation. It is even estimated that Colorado’s oil shale deposits could hold upwards of 1 trillion barrels of oil if the technology proves to be both economical and environmentally feasible.

Another source of data for consumption is the Colorado Department of Revenue’s (DOR) listing of fuel sales volumes for excise tax reporting³. While not comprehensive of all fuels and categorized differently from the EIA, DOR’s numbers provide more recent data in some areas. The gross volumes for the fiscal year ending in June 2011 (including tax-exempt sales and sales distributed out-of-state) are listed in Table IX-10 below. Jet fuel consumption includes military jet fuel within the state.

Table IX-10 Colorado Gross Fuel Volumes Consumed (fiscal year 2010-2011)

Fuel	Gasoline	Diesel	Aviation Jet Fuel	Other (alternative fuels and av. gasoline)	Total
Consumption (thousand barrels)	51396	15001	4264	587	71248
Consumption per day (thousand barrels)	140.8	41.1	11.7	1.6	195.2

Source: Colorado Department of Revenue fuel sales volumes excise tax reporting fiscal year 2010-2011.

The Regional Air Quality Council commissioned a 2011 report⁴ that examined gasoline demand in three different regions of the state: Denver-Front Range (covering the northern section of the Eastern Plains as well), Southeast CO (including Colorado Springs and Pueblo), and the Western Slope. While the study only covers gasoline, it gives a good idea of the regional breakdown of consumption; the Denver/North Front Range makes up a significant majority of demand. The data are shown in Table IX-11 below and are from 2009.

Table IX-11 Colorado Gasoline Demand – 2009 (in million barrels per day, (mbpd))

Region	Consumption (mbpd)	Percentage of total
Denver/North Front Range	96	70.6%
Southeast Colorado	24	17.6%
Western Slope	16	11.8%

Source: Energy Information Administration

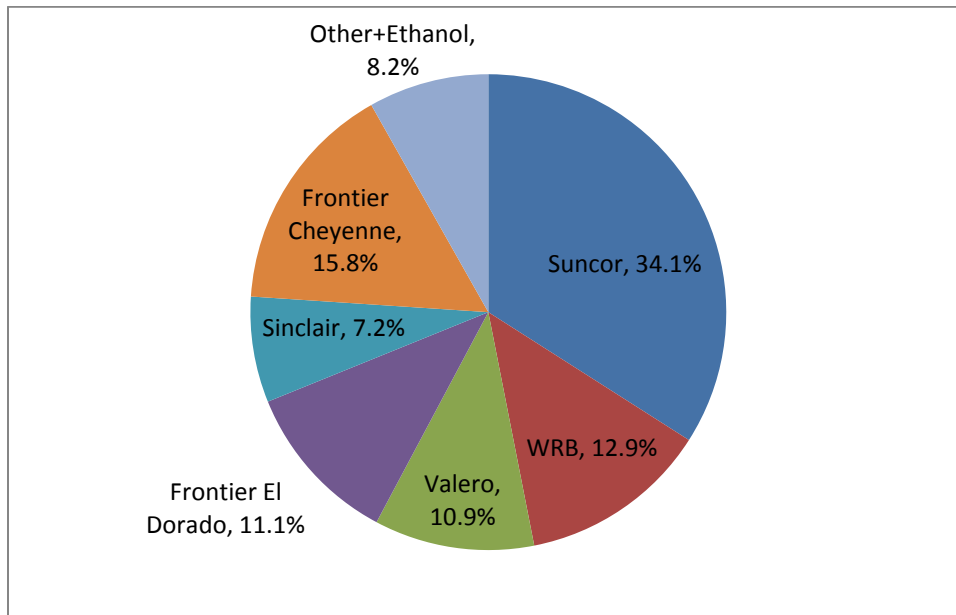
The supply chain for liquid fuels can be broken down in to three main components: refineries, pipelines, and distribution (trucks/trains and marketers). The Regional Air Quality Council’s 2011 study gives an excellent description of the refineries and pipelines contributing to Colorado’s market.

Colorado is supplied by 6 main refineries: Suncor in Commerce City, CO; WRB in Borger, TX; Valero in McKee, TX; Frontier in El Dorado, KS; Sinclair in Rawlins, WY; and Frontier in Cheyenne, WY. Others may contribute in small ways depending on market conditions. Suncor is the only in-state refinery and is the largest supplier to Colorado. The breakdown of gasoline supply share from the refineries in 2009 is shown in Figure IX-34 below.

³ <http://www.colorado.gov/cs/Satellite?c=Page&cid=1213954144067&pagename=Revenue-Main%2FXRMLayout>

⁴ “Denver/North Front Range Fuel Supply Costs and Impacts.” Regional Air Quality Council 2011. Prepared by EAI Inc. Retrieved at http://raqc.org/postfiles/reports/fuels_study/DenverNorthFrontRangeFuelSupplyCostImpacts_EAIInc_2011_REV%202.pdf.

Figure IX-34 Refinery Share of Gasoline Market



Source: Regional Air Quality Council (RAQC) Report 2011

Each of the refineries depends largely on dedicated product pipelines to ship finished products into terminals in the Denver metro area, from where they are trucked throughout the state. The capacity of these pipelines is generally not full year-round and additional products could be brought in during emergencies. However, the ability to bring in extra capacity depends on demand and sales in neighboring markets. While a significant portion of each refinery’s output comes to Colorado, further production at will may not be a consideration.

There are five product pipelines serving the Colorado liquid fuels market. Magellan LP owns a pipeline from Wichita/El Dorado, KS supplying product from the Frontier refinery in El Dorado. ConocoPhillips pipeline supplies product from the WRB refinery (a JV including ConocoPhillips) in Borger, TX as well as some product from the Valero refinery in McKee, TX. The Rocky Mountain Pipeline System (owned by Plains All American Pipeline) brings product from the Frontier Cheyenne refinery down from Wyoming. NuStar owns a separate pipeline from McKee, TX carrying products from that Valero refinery. The Denver Products/Medicine Bow pipeline, owned by Sinclair serves the Sinclair refinery in Rawlins, WY.

The 2011 Regional Air Quality Council (RAQC) report published the capacities of these pipelines and their estimated volumes in 2009. These numbers are in Table IX-12 below⁵. It should be stressed that increasing volume up to capacity is not a simple matter, as it would require taking product away from the other markets served by the refineries sourcing each pipeline.

⁵ Regional Air Quality Council Report, 2011.

Table IX-12 Estimated Pipeline Capacity – 2009 (pipelines servicing Colorado)

Pipeline	Terminus	Capacity (bpd)	2009 Peak Seasonal Volume (bpd)
Magellan LP	El Dorado, KS	60000	41154
ConocoPhillips	Borger, TX	42000	31008
NuStar	McKee, TX	38000	25433
RMPS	Cheyenne, WY	54000	23484
Sinclair	Rawlins, WY	20000	15960

While these pipelines generally serve the refineries closest to their terminus, as described above, there are two exceptions. The Rocky Mountain Pipeline System from Cheyenne is able to access products from refineries further north in Casper, WY and Billings, MT. It is also possible for product from the Gulf Coast to make it to Colorado, by traveling to the Tulsa area and then from Tulsa to El Dorado, KS and then on the Magellan pipeline from El Dorado to Colorado. Neither of these routes is used particularly often and both face pipeline restrictions further upstream.

These pipelines deliver their products to terminals where they can be sold to petroleum marketers. There is some storage of fuel at the terminals, though not a large amount as they wish to avoid basic risk just as the refiners do. Most of the terminals are in the Denver metro area, north of downtown, although there is one in La Junta (on the ConocoPhillips pipeline) and two in the Colorado Springs area (NuStar and Rocky Mountain Pipeline System). There is also the rail terminal at Colorado Fuel Manufacturers in Grand Junction. The Denver metro terminals are interconnected fairly well.

Once the refined products reach the various terminals throughout the state they are transported by truck to Colorado’s fuel marketers. Most of the marketers source their product from Colorado terminals, although some close to the Kansas, Wyoming, and New Mexico borders may also receive products from terminals in those states. According to the 2011 RAQC report, Jackson County receives nearly all of its fuel from sources in Wyoming. The entity responsible for regulating the safety of petroleum storage tanks as well as petroleum product quality throughout the state is the Colorado Department of Labor and Employment’s Oil and Public Safety Division (CDLE OPS). According to CDLE OPS’s website, there are around 2,350 retail gas stations in the state⁶. The Colorado-Wyoming Petroleum Marketers Association (CWPMMA) represents stations selling over 70% of the fuel in the state.

Implications

The effective management of liquid fuel disruptions is essential to the economy and public safety of all of Colorado’s communities. The primary vulnerabilities in the liquid fuels sector are as follows:

- International, national, and/or regional supply disruptions
- Electrical grid failures

⁵ <http://www.colorado.gov/cs/Satellite?c=Page&cid=1248095303343&pagename=CDLE-OilPublicSafety%2FCDLELayout>

- Transportation disruptions (road, rail, and pipeline)
- IT/Communications and financial services.

The 2009 Colorado Liquid Fuels Emergency Action Plan was created to encourage public/private partnerships to maintain liquid fuels status awareness, develop priorities, implement courses of action and to communicate effectively with the public when liquid fuels are disrupted. CEO is currently revising this Plan.

Smart Grid and Distributed Generation

Smart Grid Considerations in the Colorado Energy Assurance Emergency Plan (CEAEP)

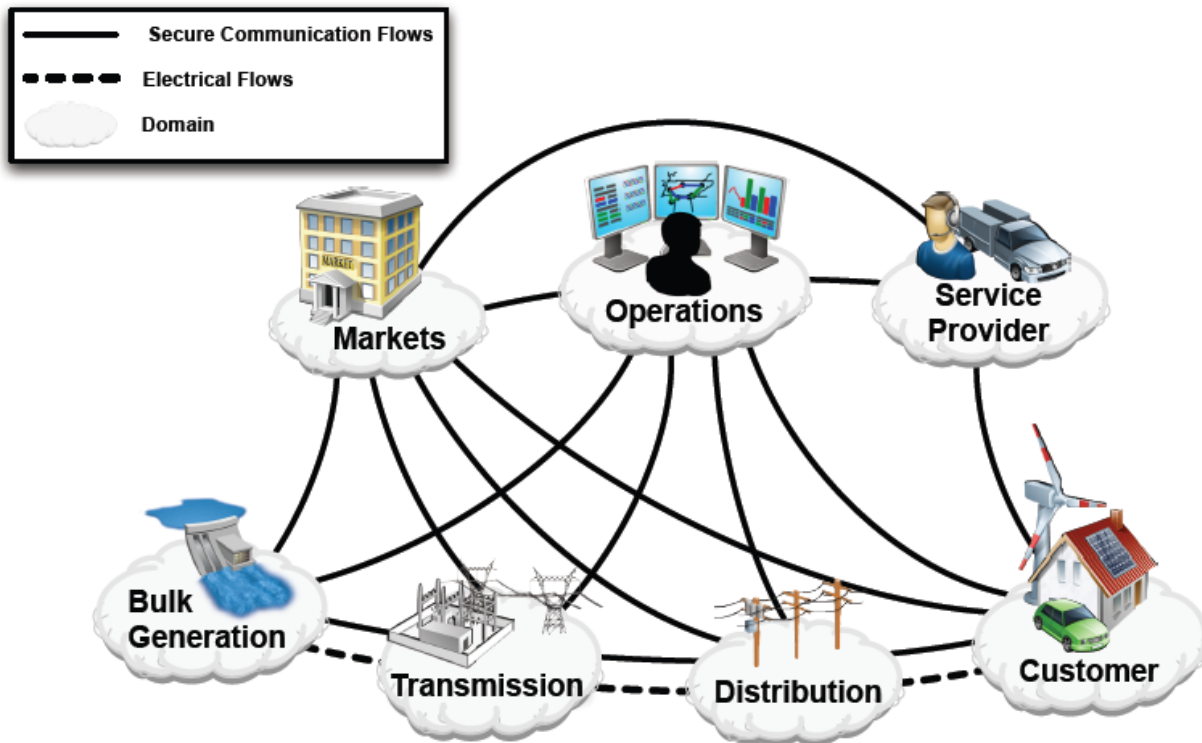
The term “smart grid” refers to a modernization of the electricity infrastructure to maintain a reliable and secure system that can meet future growth. The common goal of a smart grid is the two-way flow of electricity and information that creates an automated, widely-distributed electricity network. It can monitor, protect, and automatically optimize the operation of its interconnected elements; from both central and distributed generators, through the high-voltage transmission network and the distribution system, and ultimately to residential, commercial and industrial customers, as well as to energy storage installations.

Development of the smart grid has evolved over several years, and will continue to develop. As lessons from current projects are incorporated as improvements in future projects. The ongoing evolution of the smart grid is projected to enable utilities to collect and analyze data to deliver real-time information. This information will be used to instantly match electricity demand with supply from all available sources, incorporating both traditional generation and wind, solar and electricity storage. The ultimate objective of a smart grid is to provide utilities the means to more efficiently balance supply and demand through real-time, two-way communication at the device level.

Another key potential smart grid benefit is a more efficient integration of renewable energy resources. A properly-designed smart grid could integrate a variable energy supply and maintain system reliability by monitoring and predicting variable supply resources. It will be able to automatically bring in other power supply resources to meet demand, or reduce load to match the supply. The smart grid will use sensors such as synchrophasors and dynamic line rating systems to enhance the visibility and monitoring of the transmission grid, and to maintain and potentially improve its reliability in the presence of large variable sources of electricity. Instead of control devices operating independently based on local measurements, networked smart grid applications will analyze data from multiple devices, allowing broader and more coordinated operations that adapt to actual situations and stabilize the grid.

Figure IX-35 provides a conceptual model of the smart grid. It consists of seven domains, each of which contains many technology applications. This model was designed by electricity stakeholders in their effort to provide input on smart grid interoperability to the National Institute of Standards and Technology 1.0 for the development of the smart grid interoperability standards roadmap. The diagram is a simplified model of the multiple and complex systems of smart grid.

Figure IX-35 Smart Grid Framework



NIST Smart Grid Framework 1.0 January 2010

Source: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 (NIST SP 1108)

The vision of a fully developed smart grid within an energy assurance context is that a fully developed smart grid will provide a reliable power supply with fewer and briefer outages, higher quality power, and self-healing power systems through the use of digital information, automated control, and autonomous systems. The smart grid is resilient, but when an outage does occur, it recovers faster in emergencies and limits the extent of outages. The degree to which a smart grid project in Colorado achieves this vision will depend upon the actual smart grid applications deployed. The *State Energy Assurance Guidelines* could serve as a model which states may use to develop their Energy Assurance plans. These Guidelines were developed by the National Association of State Energy Officials (NASEO) in collaboration with the National Association of Regulatory Utility Commissioners (NARUC) and funded by DOE/OE.

State energy assurance plans can include smart grid considerations, in order to enhance energy emergency response in the short term, and reduce vulnerability and risk in the longer term. The “smart meters” that comprise the Advanced Metering Infrastructure (AMI) portion of a smart grid, have the potential to provide States with power outage information that is timelier and more accurate than otherwise possible. Smart grid characteristics such as outage detection and self-healing capabilities can, if properly deployed, improve electricity grid system response to energy emergencies. Smart grid integration of demand response and local energy resources such as renewable energy can also reduce electricity system vulnerabilities

Self-Healing Power Grid

In many states the utilities' electric distribution feeders provide service in only one direction, from the substation (source) to the customer (load). Most feeders also contain switches that allow certain customers or segments of feeders to be transferred to a different feeder during outage conditions. This switching process is manual and causes customers to be “dropped” momentarily and then “picked up” by the second feeder. Traditionally, such operations are often limited since there is usually insufficient time to analyze whether the second feeder has the capacity to serve additional electric demand. Since the number of protective devices on any given feeder has been historically limited by economic considerations, the strategy often results in the curtailment of service to customers that are served by unaffected equipment

The concept of “self-healing” means that the grid detects problems in real time, isolates the problem, and keeps the grid operating during emergencies. A deployed smart grid can augment the manual feeder switching process via a Distribution Automation (DA) capability. Distribution Automation provides an automated response to feeder line faults by using an analytical assessment, direct automatic feeder sectionalizing and restoration. After the system detects a line fault, it determines its location, and opens the nearest available switches during a tripped state of the fault-clearing re-closer or breaker. This automatically isolates the faulted segment from the rest of the feeder. Afterward, the system automatically closes switches to restore power to unfaulted distribution feeder segments. This sequence of events is considered to be “self-healing” since it occurs automatically. The validation process, which confirms the faulted distribution feeder segment is a critical step and must precede any automatic restoration. In an emergency outage situation, the self-healing feature may provide the capability to isolate the problem areas while keeping the rest of the grid operating and avoiding cascading failures. The problem areas can be repaired and restored with minimal impact on the wider area.

Distributed Generation Considerations in the Colorado Energy Assurance Emergency Plan

In Colorado, the majority of electricity is generated through large centralized facilities. The electricity produced often has to be transmitted over long distances on the way to the end customers. Lengthy transmission paths often result in power losses. One alternative to the remote generation-distant transmission model is Distributed Generation (DG). Also called onsite power generation, Distributed Generation involves producing electricity in close proximity to where it is used, often at the very same building. This enables utilities to defer or eliminate costly investments in transmission and distribution system upgrades and provides customers with better quality, more reliable energy supplies and a cleaner environment.

Microturbines

Microturbines are small combustion turbines, approximately the size of a refrigerator, which can generate outputs of 25 kW to 500 kW of electricity, and can be located on sites with space limitations for power production. Microturbines run at high speeds and, like larger gas turbines, can be used in power-only generation or in CHP systems. Microturbines offer a number of potential advantages compared to other technologies for small-scale power generation, including compact size, high efficiency and easy application in both peak demand and back-up power situations.

DG resources are typically small scale, such as solar panels on the roofs of buildings or small wind turbines. This approach reduces the amount of power lost in the transmission process. During an energy outage situation, local governments can use DG to minimize power losses to mission critical infrastructure, such as computer and communication facilities and police and fire stations. There are also distributed cogeneration sources that use natural gas-fired micro-turbines to turn generators, with the waste heat used for space or water heating, as in combined heat and power systems.

There are about 12 million DG units installed across the country, with a total capacity of about 200 GW. Most of these are back-up power units and are used primarily by customers to provide emergency power during times when grid-connected power is unavailable. Under Colorado state law, to be considered distributed generation, a project must fulfill either of the following two conditions:

- 1) To produce no more than 120% of the total on-site load,
- 2) Have a total capacity under 30 MW in the case of biomass, wind, solar photovoltaic, and geothermal, or 10 MW in the case of hydropower projects.

There is significant regional variation in the use of DG systems throughout the U.S. This is largely due to the fact that the potential benefits of DG are greater in some areas than others. In some Northeast states, for example, relatively high electricity rates, reliability concerns and DG friendly regulatory programs have encouraged comparatively high rates of DG development. But in many areas, even where DG could offer benefits, projects are often blocked by market and other barriers. There is also regional variation in the nature and impact of barriers to DG development. Overall, the

Cogeneration

Cogeneration, also called combined heat and power (CHP), is a DG technology that is gaining in popularity with local governments as an energy assurance strategy. CHP involves the use of an engine or power station to simultaneously produce electricity and useful heat. Small scale CHP applications include hotels, industrial plants, local governments and universities that redirect waste heat away from onsite power generation sources (or from other heat sources) to a different area.

Large scale CHP applications often involve utilities, and can be elaborate enough to require interconnection agreements. The state of Texas law required CHP feasibility studies as of September 2009 for all critical governmental facilities and buildings.

To meet the requirements of the Texas law, CHP systems must be able to provide all of the electricity needed for the facility's critical emergency operations for at least 14 days and at an overall efficiency exceeding 60 percent. For emergencies where the electricity grid is down for days or weeks, CHP systems are much more reliable than conventional diesel backup generators.

most commonly cited barrier to DG development is the process of interconnecting with utilities' power distribution and transmission systems. There are several economic and institutional reasons why electric utilities have not installed much DG. The economics of DG are such that financial attractiveness is largely determined on a case-by-case basis, and is very site-specific. As a result, many of the potential benefits are most easily captured by customers so that the incentives for customer-owned DG are often far greater than those for utility-owned DG.

Nevertheless, DG offers potential benefits to electric system planning and operations. On a local basis there are opportunities for electric utilities to use DG to reduce peak loads, to provide ancillary services such as reactive power and voltage support, and to improve power quality. Using DG to meet these local system needs can add up to improvements in overall electric system reliability. DG can also be used to decrease the vulnerability of the electric system to threats from terrorist attacks, and other forms of potentially catastrophic disruptions, and to increase the resiliency of other critical infrastructure sectors as defined in the National Infrastructure Protection Plan (NIPP) issued by the Department of Homeland Security, such as telecommunications, chemicals, agriculture and food, and government facilities. There are many examples of customers who own and operate facilities in these sectors who are using DG to maintain operations when the grid is down during weather-related outages and regional blackouts.

Smart Grid in Colorado

The 2010 Colorado Senate Bill 180 established a Smart Grid Task Force that produced an analysis of the costs and feasibility of transitioning the traditional grid to a secure, resilient, advanced Smart Grid. Many utilities, including those within Colorado, appear to be engaging in smart grid deployment and testing projects. However, most smart grid projects in the state of Colorado are focused on replacing traditional energy meters with smart meters rather than implementing large-scale smart grid projects. One of the most advanced projects is Xcel’s Smart Grid City initiative in Boulder where they have installed approximately 23,000 automated smart meters.

Table IX-13 Smart Grid Utility Projects 2010

Company	Project
Xcel Energy	Deploy SG system in Boulder
Black Hills/Colorado Electric Utility Company	Install 42,000 smart meters and communications infrastructure to facilitate meter reading, provide pilot for a dynamic pricing program
City of Fort Collins Utility	Installing 79,000 smart meters and in-home demand response systems
Colorado Springs Utilities	Installing AMI system
City of Fountain Utility	Install 14,600 smart meters, extend fiber optic network, deploy outage management system (partnership with Loveland, Longmont, and Fort Collins)
Delta Montrose REA	Installed 31, 000 smart meters

Source: Smart Grid Deployment in Colorado: Challenges and Opportunities, 2010. <http://cees.colorado.edu/sgreport.pdf>

Smart Grid and Distributed Generation Vulnerabilities

The ability of a distributed generation actor to provide sustained levels of required power quality during an emergency depends upon a number of factors; some of which are controllable, some are not:

- Each additional link can add a potential vulnerability to cyber attack.
- Renewable generation assets such as solar and wind are intermittent, depending upon climate conditions (e.g., the presence of enough wind pressure to consistently turn the turbine), time of day, and weather.
- A robust, secure grid connection and power lines/underground cables capable of handling the full capacity of the distributed asset on a sustained basis throughout an emergency. For example, power lines connecting a remote generation asset to the grid may not be capable of safely carrying 30%-50% more power consistently throughout the duration of an energy emergency.
- Dependability of the distributed generation asset. If a distributed generation asset is to be included in an energy emergency plan, the assumption is made that the asset will be able to perform when needed. Consumer performance standards and maintenance metrics will need to be developed in order to ensure that the asset is indeed able to perform as required in an emergency (which makes a vulnerability assessment critical). A compliance/audit process may need to be developed so that these resources can be relied upon.
- If storage devices are deployed with any distributed asset, they would need to be included in any vulnerability assessment, as their performance would be critical in ensuring a consistent power source during time of day/weather/climate situations in which a renewable generation asset is not able to perform.

The examples listed above are only a small representation of the potential challenges that would need to be assessed for inclusion in a statewide energy emergency response plan. Any assessment would need to include the current level of distributed generation assets, and more importantly, future forecasts.

Many utilities are already deploying pilot applications in targeted areas and are formulating plans to proceed with large-scale deployments soon after their pilots are complete. An accelerating pace of deployment imposes the need for the rapid development of guidance for vulnerability, preparedness, response, and mitigation.

Security profiles have proven to be a good first step in addressing vulnerabilities. A security profile is a document that contains a baseline set of security controls for a given smart grid application. By segmenting physical and cyber security guidance based on smart grid applications (and associated components), guidance can be developed incrementally. This allows, for example, an AMI security profile to be developed without simultaneously grappling

Fuel Cells

Fuel cells are similar to batteries. They can be used in a variety of applications ranging from powering cars, trucks, and buses to powering portable devices such as cell phones and laptop computers. Today, fuel cells are used most widely as a stationary source of backup power, and are often fueled with natural gas. Over the past decade, the Federal government has spent billions of dollars on hydrogen fuel cell research as part of its Hydrogen Fuel Initiative.

Hydrogen fuel cells can be used to power small hand-held devices, as well as larger devices such as portable generators used for backup power. Hydrogen fuel cells are valued because after converting the chemical energy in hydrogen to electricity, the only waste is (pure) water and heat. Hydrogen fuel cells are also prized for their high efficiency, typically 60 percent, versus traditional power sources such as coal, which deliver power at roughly 35 percent efficiency.

with other smart grid applications, such as automated data exchange. Guidance from different security profiles can be combined when utilities field multiple smart grid applications, or can be considered independently should a utility incrementally deploy their applications.

A security profile also includes a domain analysis that describes the logical architecture of the application (where security controls are associated with the components of the logical architecture). The logical architecture is kept relatively abstract to ensure applicability across a wide range of products.

Organization of security controls against logical components provides a utility with a picture of security requirements across a range of discrete products. Controls for individual components can also be quickly accessed.

The Advanced Security Acceleration Project, prepared by the Smart Grid Security Working Group under the National Institute of Standards and Technology, developed seven high-level security objectives for smart grid projects:

- 1) Ensure the availability, integrity, and (where appropriate) the confidentiality/privacy of all mission-critical elements of a smart grid application and its associated data in the face of malicious attacks or unintended adverse cyber and physical events (i.e., *security events*).
- 2) Protect the electrical system, utility personnel, the general public, and all other stakeholders (including service providers and their own services and assets) from harm caused by any security event associated with any smart grid application.
- 3) Ensure that sufficient information about a security event is available when and where it is needed to support the decision making necessary to protect (or minimize the disruption to) the mission of the affected smart grid application.
- 4) Support survivability and resiliency by continuing to fulfill critical functions (perhaps in a degraded mode that still provides essential services) during and after an attack, accident, or other adverse event.
- 5) Never allow any smart grid application or its associated technology to be used as a stepping stone or conduit for attacks on other smart grid applications, end users, external service providers, or any other interconnected entity. The weakest link of the smart grid could provide an attack vector and, consequently, the controls associated with the least important element link should be as carefully considered as those of the most important elements.
- 6) Ensure that smart grid applications will not amplify the adverse effects of any attack, accident, natural disaster, or human error.
- 7) Ensure that the security and survivability services and controls used to protect the smart grid do not provide an attack vector or incorrectly respond to malicious or benign stimuli in a manner that would create or worsen a security event.

Any security and survivability control found in a security profile should help achieve one or more of these objectives. While any individual device, component, or subsystem may not

contribute to all of these security objectives, the system as a whole must fulfill all of them with appropriate assurance.

Colorado Energy Sector Asset Database

GIS Analysis and Hazard Mapping: Critical GIS support for the EA planning process has been provided by Patrick Engineering, Inc. in the form of GIS energy sector assets database and natural hazard overlay maps, which are maps of specific natural hazard zones laid over the geographic location of major energy infrastructure assets in Colorado. The energy assets include pipeline, generating facilities, major substations, transmission networks, and major distribution networks. This GIS mapping element is considered as the Companion GIS Hazard Mapping Booklet to the CEAEP. The maps show the hazard zones county-by-county intended as a quick reference for energy asset risk and vulnerability assessment purposes.

The selected hazards include Avalanche, Flood, Wildfire, Tornado and wind, Winter Storm (ice and wind), Drought, Extreme Temperatures, and Lightning. It also compiles 2012 dollar estimates of total energy sector assets by county. In addition to the natural hazard overlay maps, a comprehensive energy sector asset database has been created. Both GIS mapping tools are for official purposes only. Table IX-14 through Table IX-17 below were selected as a sample of the risk and vulnerability assessment conducted during the EA planning process. The top twenty energy inventory asset holding counties in Colorado are listed by miles of transmission, miles of pipeline, number of substations, and number of power plants. Note the prominence of El Paso and Weld counties in each Energy Asset Inventory Rankings.

Table IX-14 Ranking by Miles of Transmission

County	Miles of Transmission	County	Miles of Transmission
Weld	858	Adams	373
Pueblo	737	Mesa	366
El Paso	696	Prowers	353
Yuma	494	Las Animas	349
Routt	436	Arapahoe	329
Morgan	425	Elbert	318
Rio Blanco	422	Garfield	316
Moffat	396	Montezuma	301
Larimer	380	Huerfano	290
Montrose	373	Kit Carson	279

Table IX-15 Ranking by Miles of Pipeline

County	Miles of Pipeline	County	Miles of Pipeline
Weld	1731	Yuma	327
Rio Blanco	1233	Arapahoe	319
Garfield	705	Morgan	312
Adams	612	Washington	253
Mesa	468	Montezuma	250
Moffat	458	La Plata	247
Las Animas	428	El Paso	213
Logan	341	Lincoln	179
Kit Carson	338	Larimer	177
Baca	329	Cheyenne	158

Table IX-16 Ranking by Number of Substations

County	Substations	County	Substations
El Paso	68	Mesa	26
Weld	62	La Plata	25
Pueblo	55	Garfield	22
Jefferson	44	Rio Blanco	21
Larimer	44	Douglas	20
Adams	38	Montezuma	20
Boulder	33	Eagle	19
Yuma	32	Logan	18
Denver	29	Montrose	18
Morgan	29	Prowers	18
Arapahoe	26	Routt	18

Table IX-17 Ranking by Number of Power Plants

County	Power Plants	County	Power Plants
Weld	14	Lincoln	5
El Paso	13	Morgan	5
Larimer	12	Prowers	5
Boulder	11	Rio Blanco	5
Adams	9	Yuma	5
Denver	7	Arapahoe	3
Mesa	7	Garfield	3
Jefferson	6	Kit Carson	3
Logan	6	La Plata	3
Montrose	6	Remaining Counties	0-2
Pueblo	6		

Costs and Strategic Approaches to Disruption

Understanding the Costs of Energy Disruption

In modern economies, all major utilities may be said to have critical infrastructural functions. However, the energy sector is particularly critical due to the high degree of energy-dependency among virtually all other sectors, and among the general public. For example, while emergency management and disaster recovery agencies have increasingly incorporated practices like backup generation, fuels stockpiling, energy efficiency, and micro-generation to decrease energy grid dependency, maintaining commercial, government, and even basic intra-organizational disaster response capabilities during a long-term and large-scale energy disruption become increasingly difficult over time.

Depending on levels of in-built redundancy among telecommunication firms, a large-scale but momentary interruption to the telecommunications sector may cause a range of impacts: momentary interruptions impacting highly redundant telecommunications networks will often produce little publicly discernible effect, but the telecommunications sector is not capable of implementing rapid grid-independence in the case of prolonged energy disruption. In the case of a longer-term energy emergency, this high degree of energy grid dependency among other critical sectors like telecommunications could potentially produce *cascade failures* in which energy-dependent sectors exceed in-house backup generation capacities and begin to suffer secondary disruption. These second and third order impacts of long-term energy supply or delivery disruptions can further compound the public and commercial impacts, and increase initial losses and recovery costs exponentially. Even in typical cases of momentary outage, telecommunications, industry, finance, information technology, and transport sectors have been disrupted.

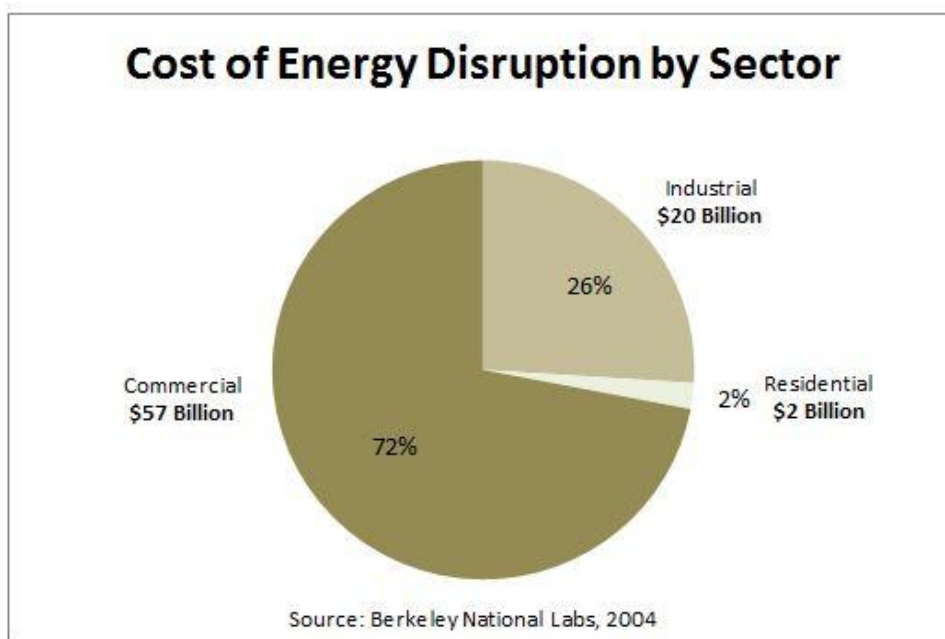
The costs associated with energy-sector disruptions are known to be significant. According to a 2005 study, losses due to power interruption across all business sectors are estimated at between \$104-164 billion annually, and costs associated with power quality problems are estimated at \$15-24 billion annually. Industrial, tech, and digital business firms lose an estimated \$5.7 billion annually due to power interruption, and among high-tech business firms, the costs of downtime due to power interruption can exceed \$1 million per minute. In 2009, the US Department of Energy estimated that power outages cost an average of \$150 billion annually, or about \$500 for every US citizen per year. Based on an interim Department of Energy report on the 2003 Northeast Blackout, statewide disruption in Colorado could incur costs estimated between \$18-49 million per hour.

Of particular interest to public-sector emergency management professionals, the residential segment constitutes 85% of retail electricity consumers in the United States, and the residential sector is most at-risk for disruption due to reliance on more extensive power distribution infrastructure than larger commercial and industrial end-users. The average duration of power interruption in the United States is seven minutes, and the vast majority of interruptions are less

than 24 hours in duration, but interruptions exceeding 24 hours are associated with vastly increased costs. Though residential consumers constitute 85% of those impacted by an electric energy disruption, it is the commercial and industrial sectors that account for the vast majority of financial losses.

The general costs of short-term ($X < 5$ minutes) interruptions substantially exceed the costs of sustained ($X > 5$ minutes) interruptions. This is a result of two dynamics: Though residential consumers are most often impacted by energy disruptions, the greatest costs to residential consumers are associated with relatively infrequent sustained interruptions, whereas the greatest costs to commercial, financial, and industrial consumers are associated with short-term interruptions and power quality issues that are more frequent.

Figure IX-36 Energy Disruption Cost



The relatively high cost of short term interruptions is primarily due to the nature of industrial and information technology processes: a momentary interruption or transient fault may produce substantial waste of industrial resources and business time as production lines must be halted and restarted due to interruption while processes are in mid-operation. Likewise, in the information technology and financial sectors, the costs of data loss and operational downtime can be substantial. For vulnerable public agencies and private-sector businesses, the costs of data loss may remain constant regardless of total downtime.

Sensitive Sectors

Business sub-sectors particularly sensitive to energy interruption include:

Digital Economy

The (DE), which is primarily composed of firms in information technology, telecommunications, research and development, electronics manufacturing, biotechnology, and finance, are characterized by their high dependency on energy-sensitive operations like data processing, data retrieval and storage, and electronic communications.

Continuous Process Manufacturing

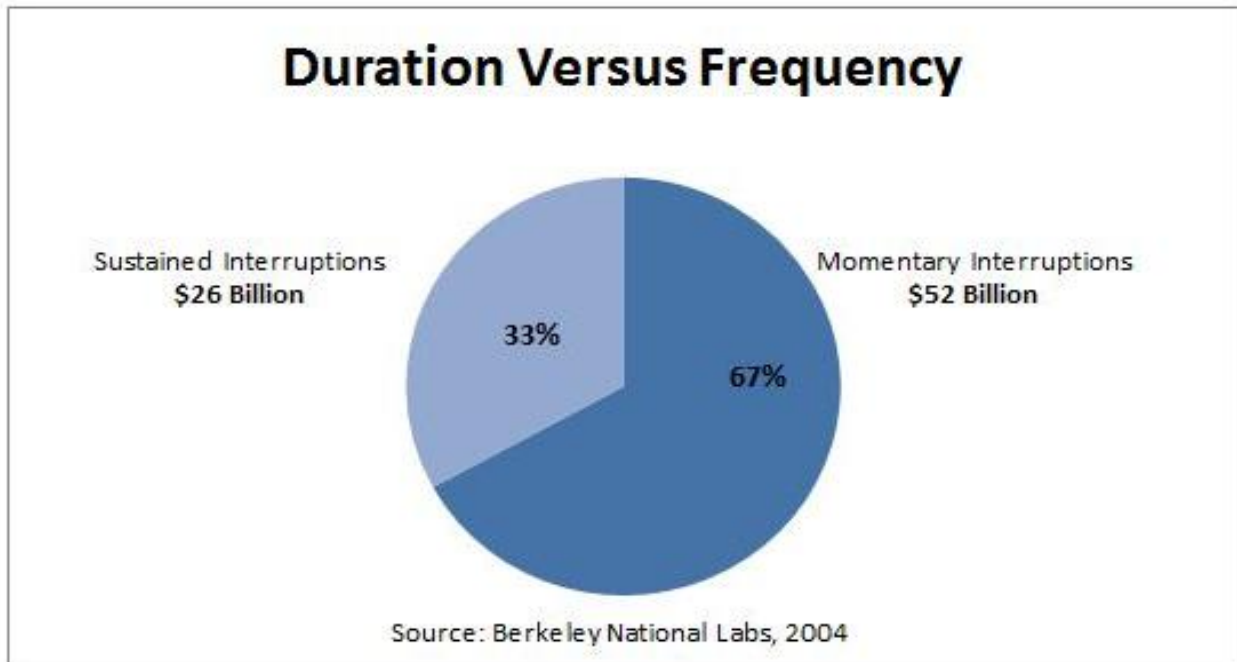
CPM, which is composed of firms with industrial facilities that operate continuously, may include paper, rubber, chemical, petroleum, glass, and metals refining and manufacturing.

Fabrication and Essential Services

(F&ES), which includes non-continuous manufacturing, utilities, transportation assets and infrastructure, mass transit, water services and treatment, liquid fuels transport, natural gas delivery and many other producers of essential goods and services. Disruptions to DE and F&ES are particularly prone to produce immediate secondary impacts on other sectors.

We can understand the general costs of energy disruption as lying along a U-curve between duration and frequency as an aggregate variable. Costs associated with short-term disruption are high due to the frequency of short-term disruption, and longer-term disruptions, though infrequent, are associated with substantial and rapidly increasing costs.

Figure IX-37 Duration vs. Frequency



When understanding the costs of energy disruptions, we can interpret costs and losses as *Primary*, or 1st Order, and *Secondary*, or 2nd, 3rd, 4th order, et cetera. Primary costs refer to direct loss of revenue and operational capability by utilities, essential government offices and private business services, and primary commercial rate-payers due to process interruption and downtime.

Secondary costs refer to losses incurred by a wider number of non-primary individuals and firms, due to interruption of service to the primary end-users. Overall costs can be evaluated not only according to specific and quantifiable economic losses, but also in the potential premiums that rate-payers would offer to utilities in order to avoid power interruption. This concept is expressed in industry studies as *willingness to pay*, or WTP. Various studies have revealed that WTP is highly variable, but significant in all markets and all sectors. Generally, levels of WTP within a national, regional, or local power market imply that vulnerability reduction measures and various types of reliability or assurance initiatives may be supported to varying degrees by rate-payers themselves.

Causes of Energy Disruption

Common circumstances behind failure to deliver energy products include disruption of distribution capacity, disruption of production capacity, and materiel supply/supply chain disruptions. Mainstream emergency management and disaster response literature classifies hazards as natural and human-caused (anthropogenic), with human-caused hazards falling further into intentional and unintentional hazard sub-categories. Natural and human-caused hazards may impact energy distribution, production, or supply chains, and may impact more than one of these categories simultaneously. The majority of natural hazards pose threats to distribution infrastructure. Ice storms and winter weather are examples of natural hazards that consistently impact transmission and/or distribution infrastructure. However, in some low probability/high impact natural disaster scenarios like a major geomagnetic storm, production, transmission, distribution, and supply chains may all be heavily impacted without significant advance warning and coordination on mitigation measures.

Human-caused hazards, whether intentional (as is the case with a physical or cyberterrorist attack), or unintentional (as is the case with infrastructure failure), may likewise impact production, distribution, or supply chains. Insufficiently analyzed and mitigated supply chain interdependencies may result in energy sector disruption even in cases for which the energy sector is not the primary target or area of vulnerability. For example, hypothetical physical attacks on global maritime transport chokepoints, or a competent, wide-ranging, and well-coordinated cyber attack, could impact the national and global transportation grids sufficient to cause major energy supply chain impacts throughout wide regional or global areas. Regardless of jurisdiction an energy assurance and energy security approach attempts to assess these kinds of interdependencies and prevent systemic impacts throughout the full spectrum of hazards.

Benefits to Energy Assurance and Security Planning

The adoption of energy assurance and energy security approaches at the state level remains a relatively recent, but potentially advantageous trend. Sound energy assurance planning and strategic energy security initiatives can support policymakers and disaster management specialists throughout all phases of the emergency management cycle. Economic costs attributable to energy interruption are significant in the United States under normal operating conditions, and would be potentially catastrophic in a case of local, state, regional, or national energy emergency. The high levels of interdependency between sectors, and the obviously critical infrastructural role that the energy sector plays in national and state economies, determine that energy assurance and energy security approaches must be integrated into mainstream emergency management planning at a variety of jurisdictional levels. Constructive all-hazards emergency management approaches, grounded in quality hazard assessments, cost-benefit calculations, and an emphasis on streamlining public-private coordination, may enable the greatest resiliency to all types of disruption at the greatest return on public and private investment.

Energy Sector Interdependencies

North American Electric Reliability Cooperation regulations require utilities to maintain at least 99.5% uptime and many aim to achieve 99.9%. With aging infrastructure, this is getting more difficult each year. A high percentage of the transmission and generation assets were installed in the 1950s and 1960s. They are still in operation well past their design life of 30-40 years. As the grid ages, more failures are expected unless mitigation measures are applied.

According to the National Association of Regulatory Utility Commissioners (NARUC), interdependency “refers to the mutual functional reliance of essential services—namely networked utility services—on other networks, utilities, services, or auxiliary nonutility system”. A disruption in one operation may affect the other, and vice versa.

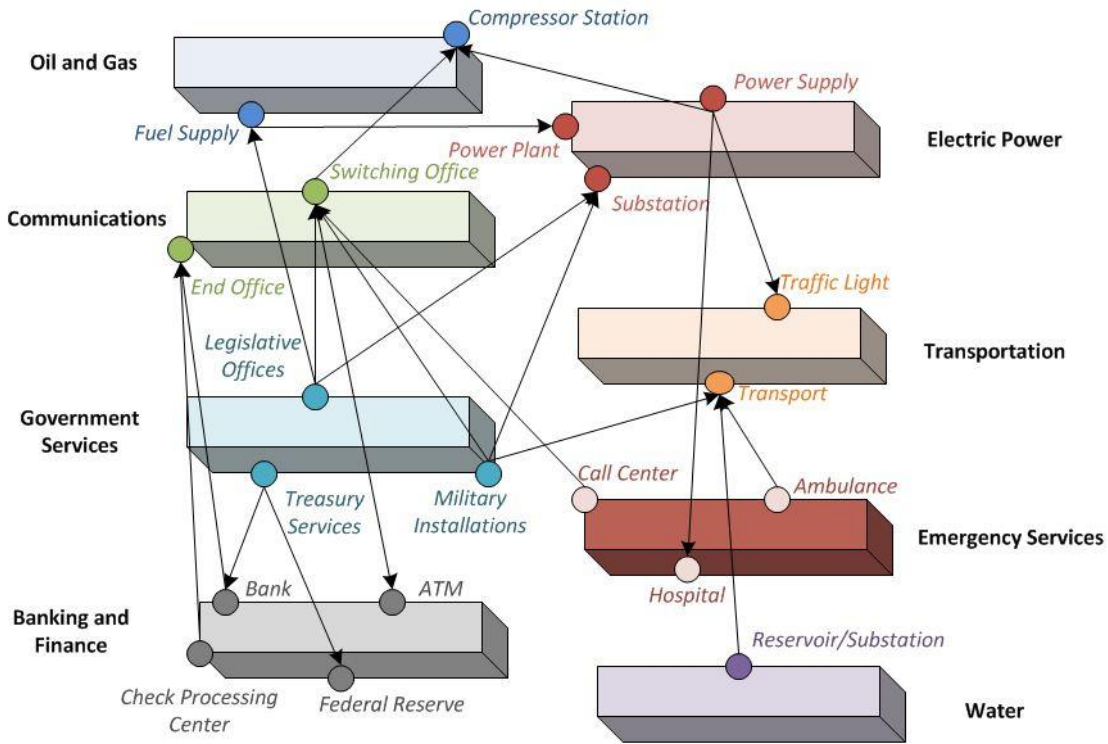
Currently, in the United States and other industrialized countries, the energy grid is a primary critical infrastructural sector. Most critical government services and business processes cannot be sustained indefinitely without an operating energy grid. In this sense, the energy sector is a keystone of critical infrastructure protection, as long-term disruptions to the energy sector may result in a series of failures in other essential sectors.

Periods of extreme weather, for example, can place enormous stresses on the electrical system. High temperatures may lead transmission lines to physically sag due to higher resistance. Demand for power increases as buildings have a need to maintain temperature set points for their occupants and equipment. This, in turn, leads to more current being transmitted on the same line which increases its resistive losses. On the other extreme, ice storms can also cause enormous damage to transmission lines due to the sheer weight of the ice. As precipitation drops onto the electrical line, it is warmed up by the resistive losses. Within a range of temperatures and wind speeds, this allows icicles to build up on the transmission line. As the storm continues to deposit precipitation, the towers holding up the lines cannot bear the enormous weights and tumble one-by-one.

Critical emergency response services, government offices, telecommunications, aviation, fuels extraction, manufacturing, healthcare, and retail industries are heavily dependent on the electrical grid. When a hazard produces a primary failure within the electrical grid of sufficient duration to outstrip backup generation capabilities, any of these and other sectors may also experience rapid failures or constraints on capability. As additional critical sectors go offline, multi-sector disruptions can compound rapidly, and capabilities are degraded.

Just as other critical sectors are highly dependent on the energy grid, the energy grid itself is an extraordinarily complex system with a number of vulnerabilities to human caused and natural hazards. Serious disruptions to the energy grid are often the result of cascade failures, which are a complex series of events which compound upon each other to produce greater impacts than any of these events could produce alone.

Figure IX-38 System Interdependencies



The NARUC has identified four types of interdependencies: physical, cyber, geographical, and institutional.

Physical Interdependencies

A physical interdependency exists when the material output of one system is used to operate another system. Electricity is used by water treatment plants to supply water to the public. If the electric power grid fails and sufficient back-up generation is not available, then the water will not be treated and delivered to the public. Physical interdependencies also exist within the energy sector. Coal and natural gas is used by electric utilities in Colorado to produce electricity. This electricity is often cycled back to the coal and natural gas providers to operate many of the facilities that they use to produce and transport the fuel. Coal plants depend on liquid fuels to transport and deliver the coal. Natural gas transportation companies may depend on electric transmission lines to operate the compressor pumps that move gas through the pipeline. The compressor is dependent on the electric utility for power; while the electric utility is dependent on the natural gas compressor. Many natural gas compressor units have their own gas-powered generators to supply power to the facility. But some of these units still rely on the electric grid and back-up, liquid fueled generators.

These physical interdependencies can be expanded further to include other public services such as telecommunications, emergency services, and government operations.

Cyber Interdependencies

Cyber interdependencies occur when multiple infrastructures use electronic information systems to transmit data. The energy sector is increasingly dependent on telecommunication and electronic information systems.

Along pipelines, supervisory control and data acquisition (SCADA) systems transfer data to control centers. Without SCADA to relay information about pipeline pressure or integrity, controllers may be forced to shut down the

flow and wait for the information system to restart. There is a commonly held belief that SCADA networks are not connected to the Internet. However, many of them are connected either directly or indirectly to the internet through virtual private networks, telephone lines, or modems. The penetration of a SCADA system could have far reaching consequences. Additionally, many liquid fuel and natural gas market centers offer Internet-based platforms to their clients to manage their business. A disruption in the electrical power grid could impact the telecommunications sector and the Internet-based trade of natural gas.

<i>Physical</i>	The operational output of one infrastructure affects the status of another, and vice versa
<i>Cyber</i>	The status of an infrastructure depends on the data transmitted through the information infrastructure
<i>Geographic</i>	A single event would be simultaneously disruptive to multiple operations within geographic proximity to one another
<i>Institutional</i>	The status of an infrastructure is dependent on another with respect to policy decisions

Geographic Interdependencies

Geographic interdependencies occur when multiple infrastructures are located in geographic proximity. Public sector facilities such as water, energy, and communications may share the same transmission or distribution corridor. For example, in western Colorado near the Piceance Basin, the White River natural gas market is located near a major natural gas power plant, storage facility, and a vast network of intra- and interstate pipelines. An incident or failure in one sector or facility may lead to subsequent failures in another.

During the 2011 Texas winter blackout, cooling pipes at coal generation facilities froze, knocking the plants offline. Natural gas compressors fed by the coal plants subsequently lost power, and gas pipelines began to freeze. As the coal plants were dependent on natural gas from these feeder pipelines to restart their generation processes, recovery was further complicated. The escalating, and eventually cascading interruption was due in part to physical and geographic interdependence.

Interdependencies between the energy sector and water utilities are another example of a geographic interdependency. Water is an essential component in the energy production process; it is used in refineries, processing plants, for resource extraction, and emissions scrubbing. Transporting water to energy producing areas is costly. Any major disruption to water delivery or water management systems may produce energy sector impacts, and disruptions to energy generation and delivery may likewise impact water delivery and management systems.

Institutional Interdependencies

Infrastructures may be linked through financial markets or influenced by regulation and deregulation. Geopolitical factors may lead to dramatic price fluctuations that impact production and supply across multiple sectors. The price or supply of petroleum, for example, may influence the production of natural gas or coal. Many large volume electricity producers can switch between oil and natural gas. Therefore, if oil prices fall then a shift in demand from gas to oil pulls gas prices down and decreases production. Institutional interdependencies are generally more subtle and difficult to identify. The problem may be further complicated by limited stakeholder coordination and information-sharing to identify interdependencies and respond to disruptions.

Interdependencies and Systemic Failures

Energy sector interdependencies can escalate failures across multiple systems. Table IX-18 illustrates some of the essential public services that may be impacted by a disruption in the energy sector.

Table IX-18 Essential Public Services Possibly Impacted by Energy Disruptions

Essential Services	Energy Source	
	Electric	Natural Gas/Oil
Banking & Finance	Financial transactions, security	Fuel for heat, generators, and facilities
Telecommunications	Switches and communication facilities, SCADA systems, repair crew communication	Fuel for heat, generators, and facilities
Transportation	Signal and control systems, fuel and goods shipment, electric powered public transportation	Fuel and lubricants for vehicles and facilities, transport of fuel and shipment of goods
Water	Control systems, lift systems, and facilities. Transportation of water, cooling and emission controls, water transport for emergency response	Fuel for treatment, heat, pumps, lift stations, and facilities.
Government	Facility HVAC, lighting, telecommunications, emergency response and protective services (EMS, police, fire)	Gas-fired HVAC, fuel/water pumping and processing

Essential Services	Energy Source	
	Electric	Natural Gas/Oil
Emergency and Protective Services	Base-to-field communications, recharging of field equipment, re-routing of individuals to facilities with electrical service	Gas-fired power generation and similar impacts to electric power system
Sanitation	Pumping and treatment	Gas-fired electrical systems, pumping and treatment

Data Source: Local Government Energy Assurance Planning (LEAP) Introduction to Energy Infrastructure Interdependencies

There are three commonly-identified types of energy infrastructure interdependency failures: cascading, escalating, and common-cause.

Table IX-19 Types of Energy Infrastructure Failure

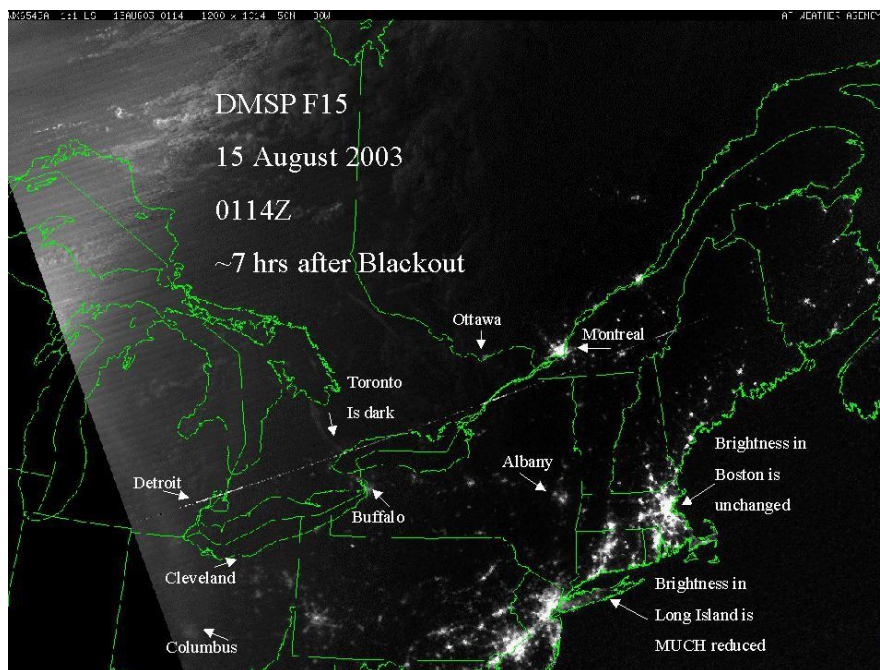
FAILURE TYPE	DESCRIPTION
Cascading	A disruption in one infrastructure causes a disruption in a second infrastructure
Escalating	A disruption in one infrastructure exacerbates an independent disruption of a second infrastructure
Common-Cause	A disruption in two or more infrastructures at the same times is the result of a common cause

Like other industries which operate through systems of complex interdependency and the multiple redundancy measures necessary to address this interdependency, major disruptions and failures in the electrical grid are rarely attributable to a single overriding factor. Instead, major disruptions are typically the result of a confluence of factors producing a series of primary and secondary impacts that are often difficult to predict and respond to. The potential for cascade failure, and the desire to prevent it, must be factored into virtually all aspects of energy emergency planning and operations.

Energy Infrastructure Interdependency Failures: Case Studies

The **two-day 2003 Northeast blackout** remains the most extensive blackout in North American history. The event, which left 50 million users without power, contributed to at least 11 deaths and caused an estimated \$6 billion in damage, was the result of a high-voltage power line in northern Ohio brushing against some overgrown trees and shutting down. This fault would normally have triggered an alarm to alert the Ohio-based utility company FirstEnergy Corporation; however, at 2:00pm on August 14, 2003, this alarm system failed. Unbeknownst to system operators, three other faults then occurred in succession, burdening other power lines with excess electrical load. At 4:05pm, the grid in northern Ohio shut down, launching a cascade of failures across southeastern Canada and eight northeastern states.

Figure IX-39 2003 Northeast Blackout



Source: <http://www.noaanews.noaa.gov/nightlights/blackout081503-7hrsafter-text.jpg>

Sagging power lines were the cause of another cascade failure leading to a blackout in the Western United States on August 10, 1996. At 3:42pm in Hillsboro, Oregon, power lines brushed against trees and shorted out. At 3:47pm in Vancouver, Washington, another power line failed. At 3:48pm, all 13 turbines of the McNary Dam on the Columbia River stopped operating. The power outages resulting from downed power lines and the loss of the McNary Dam triggered a cascade of failures across eight West Coast states. The Pacific Northwest-Pacific Southwest Intertie grid of high-voltage power lines did not have enough voltage to maintain electricity transmission, and four million people were without electricity for several hours. The Western electric grid had previously experienced a major blackout on **July 2, 1996**. It was a hot summer day, and the electricity loads in Idaho were already high. Two 345 kV lines were lost, resulting in the subsequent tripping of two Jim-Bridger units in the southern Idaho-Montana region. These

further stressed the already low voltage conditions in the Boise area, and the slow, gradual voltage decline suddenly collapsed, leading to a loss of considerable load in and around Boise, as well as the gradual tripping of transmission lines into Boise. Within seconds after the Boise collapse, the voltages on the 500 kV side of the Northwest supporting the Idaho grid had collapsed dramatically to near 300 kV. This led to the tripping of the critical California-Oregon Intertie transmission lines, causing system separation and a blackout.

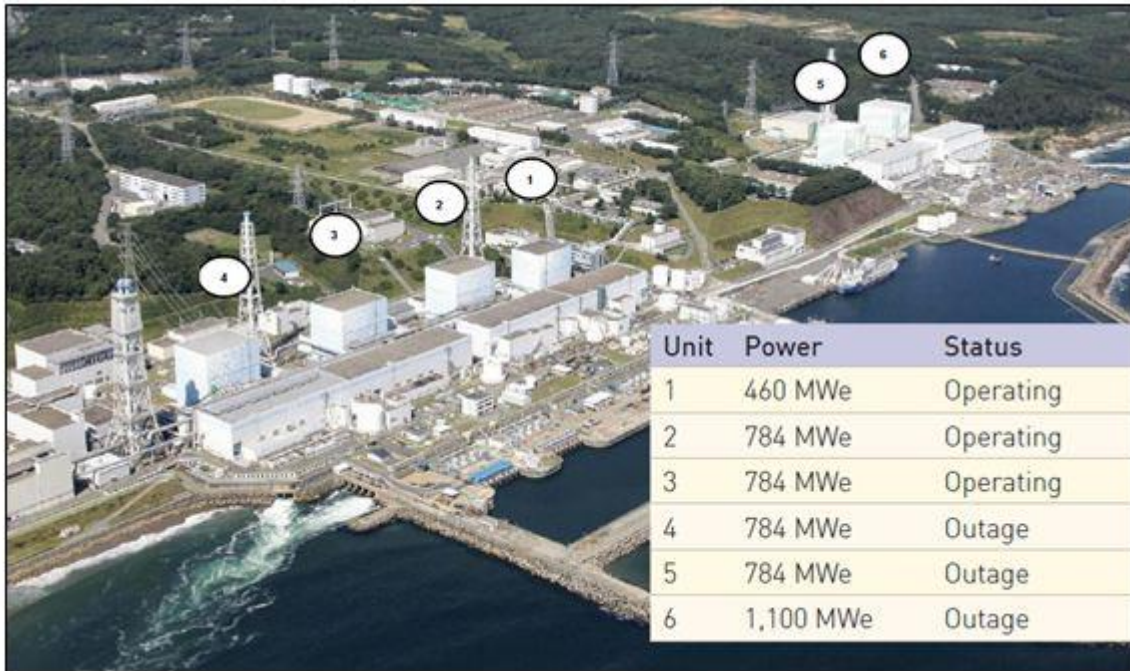
On March 13, 1989, a severe geomagnetic storm caused the collapse of Hydro-Quebec's electricity transmission system. Just after 2:44am, the electrical currents created by solar plasma striking the Earth's magnetic field found a weakness in the power grid of Quebec, tripping circuit breakers. These currents caused protective relays to sense overload conditions and lose voltage regulation. Capacitors along the entire transmission network experience power swings and a reduction of power generation until they went offline. In less than 30 seconds, Quebec lost half of its electrical power generation. Automatic load-reduction systems tried to restore a balance between the loads connected to the power grid and the massive loss of capacity now available. One by one, the load-reduction systems disconnected towns and regions across Quebec, but to no avail. Within 90 seconds, the entire Quebec power grid had collapsed. The power failure lasted nine hours.

In February 2011, Texas experienced rolling blackouts due to the extreme cold. Temperatures had fallen to the single-digits in certain cities and approximately 50 of the state's 550 power plants went down, resulting in a loss of 8,000 MW or about 12 percent of the electricity demand. An additional 12,000 MW was unavailable due to scheduled maintenance. Two coal-fired plants in Central Texas were forced offline by broken and frozen pipes. The power outages lasted anywhere from 20 minutes to over eight hours, causing significant disruptions across the state. The 911 and 311 systems became overloaded as people called to report blackouts. Several flights in and out of Austin International Airport were cancelled, and streets have been backed up due to outages at major intersections. To mitigate the effects of the blackouts, Texas imported about 300 mw from Mexico, and state officials encouraged households and businesses to conserve energy. The last time that rolling blackouts were imposed by state transmission utilities was in April 2006 during a heat wave. Despite weather reports days in advance of the extreme cold moving with this storm, plant operators were not prepared. In the early hours of February 2nd many coal plants went off-line due to frozen water pipes. As plants went off-line, this caused the natural gas in the pipelines to lose pressure as compressors had no power due to blackouts. The cold then caused gas pipelines to freeze, adding to the immediate troubles. Texas stands alone as an independent power grid. The interconnections that exist between Texas and other states are limited. Had Texas been more connected with the rest of the country, the entire Eastern interconnection would have responded to stabilize demand-supply balance in Texas and prevented the blackout.

Cascading, Escalating, and Common-Cause Failure: The Fukushima Daiichi Disaster

The events of the Fukushima Dai-ichi Nuclear Power Plant resulted from a series of equipment failures, nuclear meltdowns and the release of radioactive materials at the Fukushima Dai-ichi Nuclear Power Plant on March 11, 2011. Cascading and escalating failures followed in the wake of the Tōhoku earthquake and tsunami, as the force of both exceeded considered plant design.

Figure IX-40 Fukushima Dai-ichi Nuclear Power Plant Status Before Earthquake



The 2011 earthquake off of the Pacific coast of Tohoku was classified as a magnitude 9.0 (Mw) undersea mega-thrust earthquake. It is the most powerful earthquake to have hit Japan and one of the five most powerful recorded earthquakes in the world. The earthquake produced powerful tsunami waves, which in addition to the loss of life and destruction of infrastructure, triggered a number of nuclear accidents, namely the ongoing level 7 meltdowns (the highest level on International Atomic Energy Agency’s scale and the same rating given to accident at Chernobyl in 1986) at three reactors in the Fukushima Dai-ichi Nuclear Power Plant complex.

At the time of the earthquake, the Fukushima Daiichi Nuclear Power Plant’s reactor units 4, 5 and 6 were in shutdown for planned maintenance. The remaining units: 1, 2, and 3, shut down automatically after the earthquake. After the initial earthquake it appeared that the operating units experienced a normal reactor trip within the normal confines of the plant’s safety designs. When the three operating units (1,2 and 3) shut down, they apparently inserted control rods into the reactors. Despite the earthquake causing the facility to lose offsite power, the facility’s response to the initial seismic event was appropriate, and would likely have been effective without the additional impacts of the subsequent tsunami waves.

However, the plant’s operators were soon faced with a catastrophic and unprecedented emergency situation: Approximately 40 minutes after the earthquake, the first large tsunami wave drenched the facility, with more waves following. These waves exceeded the facility’s break walls by about 27 feet, and ended up inundating the entire plant, destroying power lines, and disconnecting Units 1 through 5 from AC electrical power causing a status known as “station blackout.” All power required for cooling the reactors and bringing them to full shutdown was lost, causing them to overheat.

In the wake of the tsunami, units 1, 2, and 3 experienced a full meltdown. Despite the best efforts of the plant operators, cooling was lost in the Unit 1 reactor after several hours, Unit 2 after 71 hours and Unit 3 after 36 hours. In the days that followed the initial disaster, the plant also suffered from explosions in Units 1, 2 and 3, as hydrogen gas was building up, and multiple fires breaking out in Unit 4.

To better understand the cascading failures which eventually led to the disaster, the Nuclear Regulatory Commission created a sequence of events during the first few days of the accident. Data and information are based on Japanese utility and official Japanese Government sources.

Unit 1 Sequence of Events	
March 11	
14:47	Earthquake, loss of offsite ac power, and plant trip
14:52	Isolation condenser operated to cool reactor
15:03	Isolation condenser stopped operating
15:37	Tsunami and total loss of ac power—SBO
15:37	Loss of ability to inject water to the reactor
~17:00	Water level below top of fuel
--:--	Partial core damage (several hours after tsunami)
March 12	
14:30	Vent primary containment
15:36	Explosion results in severe damage to the reactor building (secondary containment)

Unit 2 Sequence of Events

March 11

14:47 Earthquake, loss of offsite ac power, and plant trip

~14:50 RCIC manually operated to inject water to reactor

15:41 Tsunami and total loss of ac power at site—SBO

March 13

---:-- RCIC continued to be used to cool reactor

~11:00 Vent primary containment

March 14

13:25 RCIC stopped operating

~18:00 Water level below top of fuel

---:-- Partial core damage (approximately 3 days after tsunami)

---:-- Blowout panel open on side of reactor building

March 15

~06:00 Explosion; suppression chamber pressure decreased indicating the possibility that primary containment was damaged

Unit 3 Sequence of Events

March 11

14:47 Earthquake, loss of offsite ac power, and plant trip

15:05 RCIC manually started to inject water into reactor

15:41 Tsunami and total loss of ac power at site—SBO

March 12

11:36 RCIC stopped operating

12:35 HPCI automatically started injecting water into reactor

March 13

02:42 HPCI stopped operating

~08:00 Water level below top of fuel

---:-- Partial core damage (approximately 2 days after tsunami)

March 14

05:20 Vent primary containment

11:01 Explosion results in severe damage to the reactor building (secondary containment)

Unit 4 Sequence of Events (Unit 4 reactor was defueled)

March 11		
14:46	Earthquake and loss of offsite ac power	
15:38	Tsunami and total loss of ac power at site—SBO	
March 15		
~06:00	Explosion in reactor building	

Unit 5 & 6 Sequence of Events (Both units were shut down for periodic inspection)

March 11		
14:46	Earthquake and loss of offsite ac power	
15:41	Tsunami and total loss of ac power at site—SBO	
March 20		
14:30	Unit 5 enters cold shutdown	
19:27	Unit 6 enters cold shutdown	

Although power was restored to parts of the plant on March 20th, reactors 1 through 4, which had taken damage by floods, fires and explosions, remained non-operational. The image below is of units 1-4 following the first explosions.

Figure IX-41 Fukushima Dai-ichi Nuclear Power Plant Units 1 – 4 after explosions

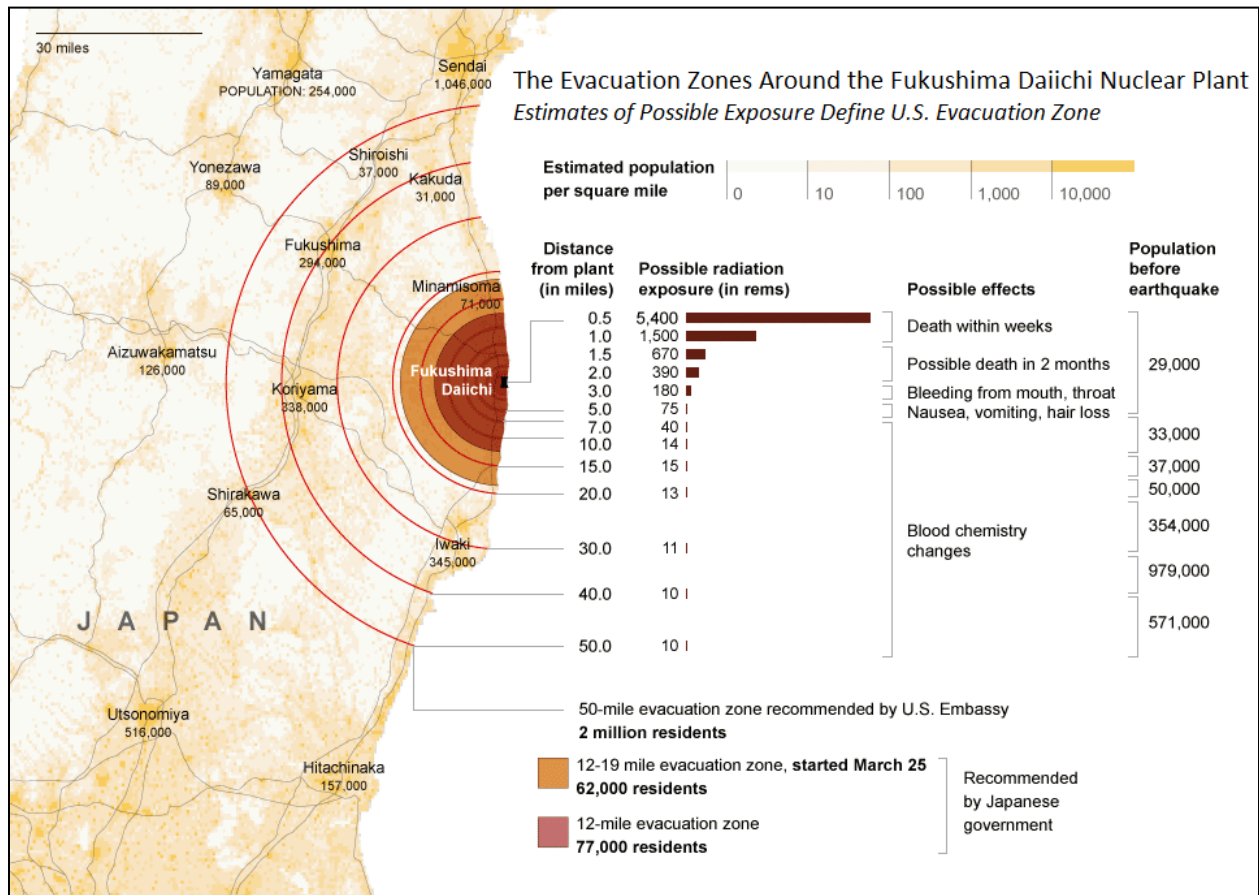


As the fires continued, authorities focused their energy on cooling efforts. On March 16th, white fumes were videotaped rising from reactor 3, suggesting its containment systems had been

breached. The Japanese Self Defense Force, firefighters, and police were called in to use water cannons to spray water on to the top of reactor 3. Spraying continued until March 23rd, with control room power restored on March 21st after a connection was made to a new power supply.

As a result of the heavy damage sustained by the plant, fears of radioactivity prompted a recommendation for an evacuation of a twelve mile radius by the Japanese government. However, based upon a recommendation by the Nuclear Regulatory Commission, the US Embassy increased its recommended areas of evacuation to a 50-mile radius for U.S. residents in Japan:

Figure IX-42 Fukushima Dai-ichi Nuclear Power Plant Evacuation Zones



While the plant operators managed to regain control of the situation in the reactors, clean-up and decontamination remain ongoing, months after the worst of the disaster.

Although no observed deaths have been documented, many have called this disaster the second-worst disaster of its kind, behind Chernobyl. James Acton, Associate of the Nuclear Policy Program at the Carnegie Endowment for International Peace stated that “Fukushima is not the worst nuclear accident ever but it is the most complicated and the most dramatic.” The cost and impacts of this disaster have been detrimental. One month after the disaster at Fukushima,

reports of workers exposed to radiation, contaminated food and the possibility of leaking reactor cores continued to stream out of Japan. In terms of financial cost, the Fukushima nuclear disaster will require Japan to spend nearly \$13 billion dollars to clean up areas in at least four prefectures which have been contaminated by radiation. However, future costs to finish the cleanup and decontamination processes will likely accrue for years or decades.

Rolling, mandatory power outages were imposed in the immediate aftermath of the crisis; it is estimated that up to five million Japanese households were affected by these outages. Tepco was forced to purchase alternative fuel sources for electrical generation and the demand for crude oil in Japan skyrocketed. Six months after the incident, Japan was still struggling to return to pre-quake power generation; in September 2011, total domestic energy production was down 7%. In response, government officials asked energy consumers to cut their power usage by 15% over the summer.

As of December 2011, only two of the Tepco's seventeen nuclear reactors were operating as the company faced a \$7.69 billion dollar net loss for the year. The future of Japan's energy sector remains uncertain. In the summer of 2011, Prime Minister Naoto Kan discussed the possibility of pushing the country towards a nuclear-free energy economy. In December 2011, Tepco was in the midst of negotiations with the Japanese government over a \$13 billion injection to help the beleaguered company repair additional reactors. The March 2011 nuclear disaster reads as a textbook example of cascading, escalating, and common-cause failures. This crisis may alter the market environment for nuclear energy in the years to come; and subsequent regulations may impact global demand for oil, gas, and renewables-based electricity providers.

High Impact Low Probability (HILP) Events

Cyberwarfare

Cyberwarfare refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare. It can be described as actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption. It is essentially the fifth domain of warfare and just as critical to military operations as land, sea, air, and space.

In 2009, President Barack Obama declared America's digital infrastructure to be a "strategic national asset," and in May 2010 the Pentagon set up its new U.S. Cyber Command (USCYBERCOM) center to defend American military networks. The European Union has set up the European Network and Information Security Agency (ENISA) with plans to significantly expand ENISA's capabilities.

The United Kingdom has also set up a cyber-security and "operations centre" based in their Government Communications Headquarters (GCHQ). In the U.S. however, Cyber Command is only set up to protect the military, whereas the government and corporate infrastructures are

primarily the responsibility respectively of the Department of Homeland Security and individual private companies. Numerous key sectors of the U.S. economy, along with that of other nations, are currently at risk, including cyber threats to public and private facilities, banking and finance, transportation, manufacturing, medical, education and government, all of which are now dependent on computers for daily operations. In 2009, President Obama stated that **"cyber intruders have probed our electrical grids."**

Cybercrime

Guardsmark, a world-wide publication noted for The Lipman Report® states http://www.guardsmark.com/library/current_report.asp?nav=4&subnav

“A persistent, ongoing problem, cybercrime generates sizable out-of-pocket costs for individual and corporate victims alike. The impact of cybercrime on people and commerce can be substantial, with consequences ranging from a mere inconvenience to devastating financial ruin. Cybercrime incidents have climbed steadily over the past decade; a recent cybercrime report claims that more than one million people become victims of cybercrime each day, and estimates the financial cost of cybercrime is larger than the combined global black market for cocaine, heroin and marijuana.”

Seemingly overnight, social networks have become the primary vehicle for terrorist recruitment, indoctrination and coordination. International terrorist organizations have shifted their Internet activity focus to social networks - and are asking users to join and support armed groups that have been included in the West's list of declared terror organizations. Shockingly, roughly 90 percent of organized terrorism on the Internet is being carried out today through social media. By using these tools, organizations are able to actively recruit new "friends" - supporters - without geographical limitations or significant risk of exposure.

The private sector owns 85 percent of all critical infrastructures in America and employs more cyber experts than the federal government. There is a great need for national legislation to require companies - who sometimes are tempted to stay silent for public and investor relations purposes - to report significant cyber breaches to law enforcement and consumers. Forty-seven states already have reporting requirements but vary greatly from state to state.

Energy Sector Cyber Invasion

The federal government admits that the electric power transmission is susceptible to Cyberwarfare. DHS works with industry to identify vulnerabilities and to help industry enhance the security of control system networks. The North American Electric Reliability Corporation (NERC) has issued a public notice that warns that the electrical grid is not adequately protected from cyber attack. It is crucial to build cyber security capabilities as the next generation of “smart grid” networks are developed.

- April 2009, reports surfaced that China and Russia had infiltrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system.
- June 2010, Stuxnet virus attacked an Iranian Nuclear Power Plant targeting the cooling system water pumps.
- May 8, 2012, officials acknowledge a campaign of cyber attacks has been targeting US natural gas pipeline operators raising security concerns about vulnerabilities in key infrastructure.

Yahoo News <http://news.yahoo.com/us-probing-cyber-attacks-gas-pipelines-030017169.html>

Massive power outages caused by a cyber attack, could disrupt the economy, distract from a simultaneous military attack, or create national trauma likened to “a digital Pearl Harbor.” It is a combination of cyber weaponry and traditional intelligence.

Power System Operations

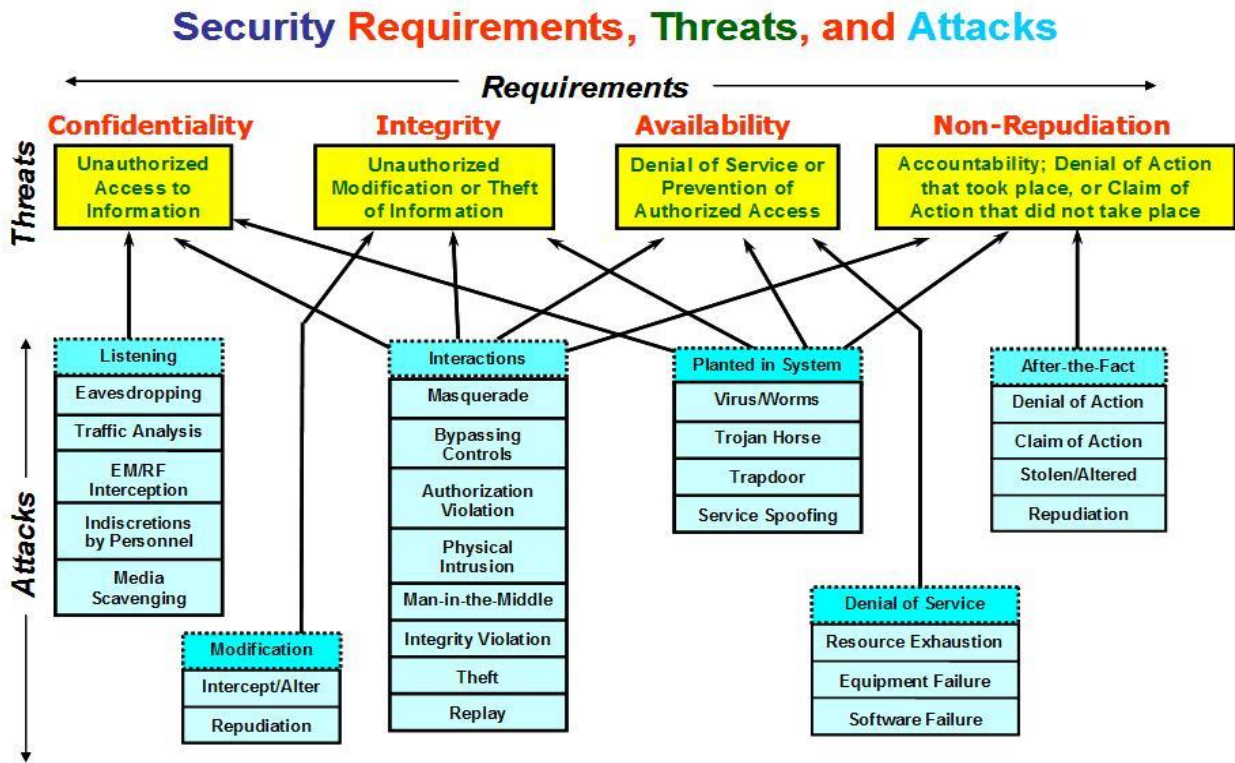
Power system operations pose many security challenges that are different from most other industries. In particular, there are strict performance and reliability requirements that are needed by power system operations.

- Operation of the power system must continue 24×7 with high availability (e.g., 99.99% for SCADA and higher for protective relaying) regardless of any compromise in security or the implementation of security measures that hinder normal or emergency power system operations.
- Power system operations must be able to continue during any security attack or compromise (as much as possible). Power system operations must recover quickly after a security attack or the compromise of an information system.
- Testing of security measures cannot be allowed to impact power system operations.

Power System Reliability

Power System Reliability is keeping electricity flowing to customers, businesses, and industry. For decades, the power system industry has been developing extensive and sophisticated systems and equipment to avoid or shorten power system outages. These existing energy management systems and equipment, enhanced and expanded, should remain as key cyber security solutions.

Figure IX-43 Core Attributes of Cyber Security



Cyber Attack Consequences and Interdependencies

The consequences of an intrusion into a smart grid system, Intelligent Electronic Device (IED)/smart device substation controller, SCADA system, controller or IED could be as severe as physical sabotage. Once a cyber intruder gains access, there is potential to:

- Shut down the SCADA system, either immediately or in a delayed manner
- Steal or alter metering and management data gathered by the SCADA system
- Shut down a substation, or any portion of a subsystem controlled by the compromised IED, either immediately or in a delayed manner
- Change protection device settings to degrade reliability of the IED and, subsequently, the electric service provided by the substation
- Gather control and protection information that could be used in a subsequent attack
- Change or perturb the data in such a manner as to trigger an inappropriate action by an IED
- Plant malicious code that could later trigger a delayed or coordinated attack
- Use the SCADA system as a backdoor into the corporate IT system to obtain customer credit and personal identity information used in electronic theft

Cyber security experts have demonstrated that certain customer-premise located "smart meters" can be successfully attacked, and the impact of such attacks includes the ability to disrupt the electricity grid. In addition, certain control systems, if exploited, could result in serious damages

and disruption. On March 2007, the U.S. Department of Defense launched an experimental cyber attack that caused a generator to self-destruct. The experiment was conducted in the Department of Energy Idaho Lab, where a replica of a power plant control system was hacked, making a generator shake and shut down in smoke. This kind of attack, coordinated in a large scale could damage the electric infrastructure for months.

Another concern with smart grid deployments is the new intersection between utilities networks and home area networks as a result of smart metering, as criminals could leverage the utilities network to break into home networks or vice versa. A concern expressed by some Colorado Utilities is Smart Grid technologies collect and use significant amounts of customer usage data that could be used by criminal elements to track residential and business customer patterns; for example: sleep schedules, Internet usage, personal traffic habits, etc.

The U.S. Central Intelligence Agency (CIA) reported that cyber attacks have caused power outages that affected multiple cities outside the United States. In a written statement provided to Thomas Clayborn of Information Week, CIA senior analyst Tom Donahue confirmed

"We have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands. We suspect, but cannot confirm, that some of these attackers had the benefit of inside knowledge. We have information that cyber attacks have been used to disrupt power equipment in several regions outside the United States. In at least one case, the disruption caused a power outage affecting multiple cities. We do not know who executed these attacks or why, but all involved intrusions through the Internet."

Cybersecurity industry experts theorize that the prospect of cyber attacks crippling multicity regions within the United States prompted the CIA to go public with this classified information.

According to the 2009 report *"In the Crossfire: Critical Infrastructure in the Age of the Cyber War"*, critical infrastructure (electricity, gas, water) information technology security executives estimated the average cost to utilities of 24 hours of downtime from a cyber incident to be \$6.3 million. Apart from cost, the most widely feared loss from attacks is damage to reputation, followed by the loss of personal information about customers. The effects of a cyber attack on energy infrastructure stretch beyond the utility's operations.

The Georgia Tech *Emerging Cyber Threats* 2011 Report indicates that a primary threat of cyber attack is the disconnection of power for a large segment of the population, and the disabling of infrastructure devices, requiring a physical visit to every device to reconnect power. There is also an economic threat in the form of power theft by sophisticated criminals who exploit the utilities' increased connection to the internet.

A cyber attack on a utility control system may have effects beyond those of the attacked infrastructure itself. Infrastructures are interdependent, which means that a failure in a utility

infrastructure will have cascading impacts on almost all industries in a community, because all industries require electrical power in some manner. Infrastructure continuity disruption can also become an economic disaster. A sustained loss of electric power, for example, may cause economic activity to come to a near halt.

The consequences of infrastructure disruptions are complicated and difficult or impossible to measure in many cases and may vary greatly in their consequences. An outage at a single generator during a period with adequate reserve capacity is unlikely to disrupt service. On the other hand, a large blackout that lasts a long time will have larger consequences that affect nearly all infrastructures and individuals. The Northeast Blackout of 2003 provides an example of the impact on extended energy outages. This limited blackout affected more than 55 million people, effectively shut down business, transportation, cities and schools, caused 11 deaths and cost an estimated \$6 billion in lost production. While that blackout was due to a confluence of non-malicious events, similar consequences might be achievable by a large-scale, coordinated, cyber attack. Advanced Information and communication technologies are also driving improvements in multiple public sector services, including eGovernment, Cloud Computing, Telehealth, Intelligent Transportation Systems and Positive Train Control. As these systems are heavily reliant upon electricity, extended outages from a major cybersecurity incident can have a devastating effect on these and other sectors of an economy.

- **eGovernment:** The use of information and communication technologies to promote more efficient government by allowing better delivery of public services, improved access to information and increased accountability of governments to its citizens
- **Intelligent Transportation Systems:** Integrated information, telecommunications and computer based technologies used to make infrastructure and vehicles safer, smarter and interconnected
- **Positive Train Control:** Integrated command, control, communications, and information systems for controlling train movements with safety, security, precision, and efficiency
- **Telehealth:** Delivery of health-related services and information via telecommunications and information technology devices

Confidentiality and Privacy of Customers

As the Smart Grid reaches into homes and businesses, and as customers increasingly participate in managing their energy, confidentiality and privacy of their information has increasingly become a concern. Unlike power system reliability, customer privacy is a new issue.

The Smart Grid Vulnerability Assessment

As with any assessment, a realistic analysis of the inadvertent errors, acts of nature, and malicious threats and their applicability to subsequent risk-mitigation strategies is critical to the overall outcome. The Smart Grid is no different. It is recommended that all organizations take a realistic view of the hazards and threats and work with national, regional, and local authorities as

needed to glean the required information, which, it is anticipated, no single utility or other Smart Grid participant would be able to assess on its own. Table IX-20 summarizes the categories of adversaries to information systems. These adversaries need to be considered when performing a risk assessment of a Smart Grid information system.

Despite the very real threat from state-sponsored cyber attacks and mass coordinated attacks, the most serious threat is from internal sources, whether intentional or unintentional. A major concern for the utilities industry is the insider threat, whereby disgruntled employees utilize cyber tactics to defraud utilities or perhaps, cause power outages. The human factor must always be considered the weakest element within any security posture. Failure in, lack of, inadequacies or deficiency in policies and procedures can lead to security risks. Inadequately trained workforce will not be aware of the policies and procedures necessary to secure organizational information and equipment, resulting in the potential for weaknesses to be exploited

Table IX-20 Categories of Adversaries to Information Systems

Adversary	Description
Nation States	State-run, well organized and financed. Use foreign service agents to gather classified or critical information from countries viewed as hostile or as having an economic, military or a political advantage.
Hackers	A group of individuals (e.g., hackers, phreakers, crackers, trashers, and pirates) who attack networks and systems seeking to exploit the vulnerabilities in operating systems or other flaws
Terrorists/ Cyberterrorists	Individuals or groups operating domestically or internationally who represent various terrorist or extremist groups that use violence or the threat of violence to incite fear with the intention of coercing or intimidating governments or societies into succumbing to their demands
Organized Crime	Coordinated criminal activities including gambling, racketeering, narcotics trafficking, and many others. An organized and well-financed criminal organization
Disgruntled Employees	Angry, dissatisfied individuals with the potential to inflict harm on the Smart Grid network or related systems. This can represent an insider threat depending on the current state of the individual’s employment and access to the systems
Careless or poorly trained employees	Those users who, either through lack of training, lack of concern, or lack of attentiveness pose a threat to Smart Grid systems. This is another example of an insider threat or adversary

Vulnerability Classes

The NISTR 7628 Guidelines for Smart Grid Cyber Security lists five classes of potential vulnerabilities with descriptions of specific areas that can make an organization vulnerable as well as the possible impacts to an organization should the vulnerability be exercised. NISTR

7628 defines a vulnerability class as a category of weakness which could adversely impact the operation of the electric grid. “Vulnerability” is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

The following potential vulnerabilities in Smart Grid infrastructure were created from many sources of vulnerability information, including NIST 800-82, *Guide to Industrial Control Systems Security*, and 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*, Open Web Application Security Project (OWASP) vulnerabilities, National Vulnerability Database Common Weakness Enumeration (CWE) vulnerabilities, attack documentation from Idaho National Laboratory (INL), input provided by the NIST CSWG Bottom-Up group, and the North American Electric Reliability Corporation Critical Infrastructure Protection Standards (NERC CIP) standards. However, the list is not exhaustive. Rather, it is just a starting point for more detailed vulnerability identification.

People, Policy & Procedure

Policies and procedures are the documented mechanisms by which an organization operates, and *people* are trained to follow them. Policies and procedures lay the groundwork for how the organization will operate. This section discusses cases where a failure in, lack of, or deficiency in policies and procedures can lead to security risks for the organization. An organization’s policies and procedures are often the final protective or mitigating control against security breaches, and those policies and procedures should be examined closely to ensure that they are consistent with both the inherent business objectives and with secure operations. Colorado utilities believe that Phishing, human/social engineering attacks tend to be more likely infiltration points than manufacturer introduced malware. This is especially true during a high stress or emergency situation when security protocols could be inadvertently relaxed or compromised to get back to business as usual.

Platform Software/Firmware Vulnerabilities

Software and firmware are the programmable components of a computing environment. Errors or oversights in software and firmware design, development, and deployment may result in unintended functionality that allows attackers or other conditions to affect, via programmatic means, the confidentiality, integrity, and/or availability of information. These errors and oversights are discovered and reported as vulnerability instances in platform software and firmware. Discovery and reporting of vulnerability instances occur continuously and the Common Vulnerability and Exposures (CVE) specification establishes a common identifier for known vulnerability instances. [§6.6-5] The Common Weakness Enumeration (CWE) [§6.6-4] and the Vulnerability Categories defined by OWASP [§6.6-1] are two taxonomies which provide descriptions of common errors or oversights that can result in vulnerability instances. Using the CWE and OWASP taxonomies as a guide this subsection describes classes and subclasses of vulnerabilities in platform software and firmware1.

Platform Vulnerabilities

Platforms are defined as the software and hardware units, or systems of software and hardware, that are used to deliver software-based services. The platform comprises the software, the operating system used to support that software, and the physical hardware. Vulnerabilities arise in this part of the Smart Grid network due to the complexities of architecting, configuring, and managing the platform itself. Platform areas identified as being vulnerable to risk include the security architecture and design, inadequate malware protection against malicious software attacks, software vulnerabilities due to late or nonexistent software patches from software vendors, an overabundance of file transfer services running, and insufficient alerts from log management servers and systems.

Network

Networks are defined by connections between multiple locations or organizational units and are composed of many differing devices using similar protocols and procedures to facilitate a secure exchange of information. Vulnerabilities and risks occur within Smart Grid networks when policy management and procedures do not conform to required standards and compliance policies as they relate to the data exchanged. Network areas identified as being susceptible to risk and with policy and compliance impacts are: data integrity, security, protocol encryption, authentication, and device hardware.

Types of Cyber Attacks

The Georgia Tech Report identified the further proliferation and sophistication of botnets - collections of software agents that run automatically to compromise large numbers of machines for malicious activity including spreading spam, stealing log-in credentials and personal information or distributing malware to others, attacks on pervasive devices such as "smart meters" and social networking - as three top trends in cyber attacks. The report highlights smart grid security and privacy issues and reveals the existence of an active community that is specifically targeting power systems. Complicating traditional cyber defense tactics is the fact that cyber criminals now have automated tools capable of releasing very large volumes of malware with extreme variety and sophisticated features.

Cyber Security Objectives

For decades, power system operations have been managing the reliability of the power grid, in which power *availability* has been the primary requirement, with information integrity as a secondary but increasingly critical requirement. Confidentiality of customer information is also important in the normal revenue billing processes and for privacy concerns.

- **Availability** is the most important security objective for power system reliability. The time latency associated with availability can vary from sub-4 milliseconds for protective relaying,

to hours and days for collecting longer term data. A loss of *availability* is the disruption of access to or use of information or an information system.

- **Integrity** for power system operations includes assurance that data has not been modified without authorization, the source of data is authenticated, the time stamp associated with the data is known and authenticated, and the quality of data is known and authenticated. A loss of *integrity* is the unauthorized modification or destruction of information
- Confidentiality is the least critical for power system reliability. However, confidentiality is becoming more important, particularly with the increasing availability of customer information online

Cyber Security Preparedness & Defense

The security defense strategies listed below are an amalgam of ‘best practices’ culled from several sources in order to develop a set of security requirements that address the needs of utilities and Smart Grid projects:

Best Practices identified in Smart Grid

- **Access Control:** The focus of access control is ensuring that resources are accessed only by the appropriate personnel, and that personnel are correctly identified. Mechanisms need to be in place to monitor access activities for inappropriate activity.
- **Awareness and Training:** Smart Grid information system security awareness is a critical part of Smart Grid information system incident prevention. Implementing a Smart Grid information system security program may change the way personnel access computer programs and applications, so organizations need to design effective training programs based on individuals’ roles and responsibilities.
- **Audit and Accountability:** Periodic audits and logging of the Smart Grid information system need to be implemented to validate that the security mechanisms present during Smart Grid information system validation testing are still installed and operating correctly. These security audits review and examine a Smart Grid information system’s records and activities to determine the adequacy of Smart Grid information system security requirements and to ensure compliance with established security policy and procedures. Audits also are used to detect breaches in security services through examination of Smart Grid information system logs. Logging is necessary for anomaly detection as well as forensic analysis.
- **Security Assessment and Authorization:** Security assessments include monitoring and reviewing the performance of Smart Grid information system. Internal checking methods, such as compliance audits and incident investigations, allow the organization to determine the effectiveness of the security program. Finally, through continuous monitoring, the organization regularly reviews compliance of the Smart Grid information systems. If deviations or nonconformance exist, it may be necessary to revisit the original assumptions and implement appropriate corrective actions.
- **Configuration Management:** The organization’s security program needs to implement policies and procedures that create a process by which the organization manages and

documents all configuration changes to the Smart Grid information system. A comprehensive change management process needs to be implemented and used to ensure that only approved and tested changes are made to the Smart Grid information system configuration. Smart Grid information systems need to be configured properly to maintain optimal operation. Therefore, only tested and approved changes should be allowed on a Smart Grid information system. Vendor updates and patches need to be thoroughly tested on a non-production Smart Grid information system setup before being introduced into the production environment to ensure that no adverse effects occur.

- **Continuity of Operations:** Addresses the capability to continue or resume operations of a Smart Grid information system in the event of disruption of normal system operation. The ability for the Smart Grid information system to function after an event is dependent on implementing continuity of operations policies, procedures, training, and resources. The security requirements recommended under the continuity of operations family, provide policies and procedures for roles and responsibilities, training, testing, plan updates, alternate storage sites, alternate command and control methods, alternate control centers, recovery and reconstitution and fail-safe response.
- **Identification and Authentication:** The process of verifying the identity of a user, process, or device, as a prerequisite for granting access to resources in a Smart Grid information system.
- **Information and Document Management:** Generally a part of the organization records retention and document management system. Digital and hardcopy information associated with the development and execution of a Smart Grid information system is important and sensitive, and need to be managed. Smart Grid information system design, operations data and procedures, risk analyses, business impact studies, risk tolerance profiles, etc., contain sensitive organization information and need to be protected. This information must be protected and verified that the appropriate versions are retained.
- **Incident Response:** Entails the preparation, testing, and maintenance of specific policies and procedures to enable the organization to recover the Smart Grid information system's operational status after the occurrence of a disruption.
- **Smart Grid Information System Development and Maintenance:** Security is most effective when it is designed into the Smart Grid information system and sustained, through effective maintenance, throughout the life cycle of the Smart Grid information system. Maintenance activities encompass appropriate policies and procedures for performing routine and preventive maintenance on the components of a Smart Grid information system. This includes the use of both local and remote maintenance tools and management of maintenance personnel.
- **Media Protection:** Policy and procedures for limiting access to media to authorized users. Security measures also exist for distribution and handling requirements as well as storage, transport, sanitization (removal of information from digital media), destruction, and disposal of the media. Media assets include compact discs; digital video discs; erasable, programmable read-only memory tapes; printed reports; and documents.

- **Physical and Environmental Security:** Encompasses protection of physical assets from damage, misuse, or theft. Physical access control, physical boundaries, and surveillance are examples of security practices used to ensure that only authorized personnel are allowed to access Smart Grid information systems and components. Environmental security addresses the safety of assets from damage from environmental concerns.
- **Planning:** The purpose of strategic planning is to maintain optimal operations and to prevent or recover from undesirable interruptions to Smart Grid information system operation. The types of planning considered are security planning to prevent undesirable interruptions, continuity of operations planning to maintain Smart Grid information system operation during and after an interruption, and planning to identify mitigation strategies.
- **Security Program Management:** Lays the groundwork for securing the organization's enterprise and Smart Grid information system assets. Security procedures define how an organization implements the security program.
- **Security Personnel:** Addresses security program roles and responsibilities implemented during all phases of staff employment, including staff recruitment and termination. The organization screens applicants for critical positions in the operation and maintenance of the Smart Grid information system. The organization may consider implementing a confidentiality or nondisclosure agreement that employees and third-party users of facilities must sign before being granted access to the Smart Grid information system. The organization also documents and implements a process to secure resources and revoke access privileges when personnel terminate.
- **Smart Grid Information Systems and Services Acquisition:** Covers the contracting and acquiring of system components, software, firmware, and services from employees, contactors, and third parties. A policy with detailed procedures for reviewing acquisitions should reduce the introduction of additional or unknown vulnerabilities into the Smart Grid information system.
- **Smart Grid Information System and Communication Protection:** Consists of steps taken to protect the Smart Grid information system and the communication links between Smart Grid information system components from cyber intrusions.
- **Smart Grid Information System and Information Integrity:** Maintaining a Smart Grid information system, including information integrity, increases assurance that sensitive data have neither been modified nor deleted in an unauthorized or undetected manner.

Each utility deploys its own cybersecurity measures, technologies and policies. It is not the intent of the Plan to be prescriptive in addressing vulnerabilities or attacks. Many security measures and technologies for utilities are still in the early adopter phase, as organizations seek to defend their infrastructure from compromise by malware. Utilities are beginning to increase work around authentication, encryption and ensuring the integrity of their computing infrastructure. They are also deploying scalable, difficult-to-detect, automated analysis system to obtain actionable malware intelligence and leverage the intelligence in meaningful ways.

However, there is general recognition in the industry that there is still a long way to go in terms of developing comprehensive, formal security plans and procedures. There is increasing agreement among utility industry participants that cybersecurity requires a community-based defense approach that includes collaboration between utilities, government, technology vendors and security researchers. Sharing of intelligence on the overall "threatscape" is a key component. Cyber security is a complex issue that requires leaders in sharing of information between utility industry leaders. Government organizations that possess classified information about potential threats will need to regularly share this actionable intelligence with the private sector in order to effectively defend against cyber attacks.

To address the increased vulnerabilities associated with Smart Grid deployments, the Energy Independence and Security Act of 2007 (EISA) provided the National Institute of Standards and Technology (NIST) and Federal Energy Regulatory Commission (FERC) with responsibilities related to coordinating the development and adoption of smart grid guidelines and standards. The U.S. Government Accountability Office (GAO) in turn was tasked with assessing the extent to which NIST developed smart grid cyber security guidelines; evaluate the Federal Energy Regulatory Commission's (FERC) approach for adopting and monitoring smart grid cybersecurity and other standards and identify challenges associated with smart grid cyber security.

In its January 2011 Electricity Grid Modernization report to the U.S. Congress, GAO indicated that NIST's August 2010 version of smart grid cybersecurity guidelines had addressed key cybersecurity elements, such as an assessment of cybersecurity risks associated with smart grid systems and the identification of security requirements (i.e., controls) essential to securing such systems. However, GAO's report found that NIST did not address the risk of attacks that use both cyber and physical means. Although NIST officials responded to the GAO report by committing to update the NIST guidelines to address the missing elements, and have drafted a plan to do so, the plan and schedule are still in draft form. GAO's position is that until the missing elements are addressed, there is an increased risk that smart grid implementations will not be secure as otherwise possible.

The GAO report identified six key challenges to securing smart grid systems:

- Aspects of the regulatory environment may make it difficult to ensure smart grid systems' cyber security.
- Utilities are focusing on regulatory compliance instead of comprehensive security.
- The electric industry does not have an effective mechanism for sharing information on cyber security.
- Consumers are not adequately informed about the benefits, costs, and risks associated with smart grid systems.
- There is a lack of security features being built into certain smart grid systems
- The electricity industry does not have metrics for evaluating cyber security.
- The following areas need to be addressed in follow-on CSWG activities.

In 2010, FERC began a process to consider an initial set of smart grid interoperability and cybersecurity standards for adoption, but has not developed a coordinated approach to monitor the extent to which industry is following these standards. While EISA gives FERC authority to adopt smart grid standards, it does not provide FERC with specific enforcement authority. This means that standards will remain voluntary unless regulators are able to use other authorities to enforce them. Additionally, FERC has not developed an approach coordinated with other federal, state and local regulators to monitor whether industry is following the voluntary smart grid standards it adopts.

In recent testimony before a Senate Committee, FERC's Joe McClelland described the current gaps in coverage in grid protections and offered suggestions to address them. He indicated that FERC currently does not have sufficient authority to require effective protection of the grid against cyber or physical attacks. Currently, the Commission's jurisdiction and reliability authority is limited to the "bulk power system," as defined in the Federal Power Act (FPA). The current interpretation of a "bulk power system" also excludes some transmission and all local distribution facilities, including virtually all of the grid facilities in certain large cities, thus precluding Commission action to mitigate cyber or other national security threats to reliability that involve such facilities and major population areas. He also expressed his opinion that the current regulatory process is too slow; and the procedures used by NERC do not provide an effective and timely means of addressing urgent cyber or other national security risks to the bulk power system, particularly in emergency situations. Certain circumstances, such as those involving national security, may require immediate action, while the reliability standard procedures take too long to implement efficient and timely corrective steps.

In Colorado there appears to be an informal network amongst some utilities staff for information sharing regarding cyber attacks, and Information Security product vendors form a pseudo information sharing environment. However, there is no formal information sharing network between the utilities and State or Federal agencies. The Colorado Division of Emergency Management does not receive reports on cyber attacks on utilities nor do they maintain a log of electric power outages or disruptions unless the event is a state declared event in which "WebEOC", a software system designed for disaster tracking, is used. This issue is one highlighted under Potential Initiatives in the Mitigation Action Plan table located in Book 2 - Mitigation Strategy.

Colorado Utilities indicate that they are comfortable with sharing information with State and Federal regulators, however, they are not comfortable with the potential for misinformation to be disseminated through the rapid speed of social and media networks and how that information is used can create bad public relations for the utilities.

The Colorado Energy Office recognizes the many initiatives underway to develop national standards or guidelines. Outcomes of these or other relevant initiatives may be incorporated into the Plan as a normal course of annual monitoring and updating of the Plan.

Recommendations

- Monitor NIST Cyber Standards and associated Grid Reliability legislation
- Participate in a Colorado Cyber Security Energy Focus Working Group
- Attend Cyber Security Conferences and Training opportunities

Solar Weather

Introduction

Solar Weather refers to the conditions and phenomena in space and specifically in the near-earth environment that may affect space assets or space operations. It is the conditions on the sun and in the solar wind, magnetosphere, ionosphere, and thermosphere that can influence the performance and reliability of space-borne and ground-based technological systems and endanger human life or health. It is influenced by phenomena such as solar flare activity - sunspots, ionospheric variability – planetary wave and tidal interaction, energetic particle events – coronal and interplanetary shock, and geophysical events –large scale volcanoes, tsunamis, extreme weather, and geomagnetic Storms (GMS) caused from solar Coronal Mass Ejections (CME). CME shock waves create solar energetic particles (SEPs), which are high-energy particles consisting of electrons and coronal and solar wind ions (mainly protons). When CMEs head towards the Earth, these geomagnetic storms create disturbances that affect the Earth’s magnetic field, which are referred to as Geomagnetic Disturbances (GMD).

<http://www.oecd.org/dataoecd/57/25/46891645.pdf>

GMS Characteristics

The force of geomagnetic field disturbances is measured by the magnitude of magnetic field change measured in NanoTeslas per minute (nT/min). An nT is one billionth of a Tesla, which is the International System of Units (SI) derived unit of magnetic flux density – the change of volt-seconds measured in the coils of a fluxmeter. Gamma is the non-SI unit of measure equal to a NanoTesla. Terrestrial effects of space weather events are determined by several coronal mass ejection (CME) variables - which include particle magnitudes, velocity and polarization with respect to the earth’s magnetosphere. An unfortunate combination of these variables can lead to extreme geomagnetic disturbances on earth – the most famous being the Carrington Event of 1859. NOAA’s Space Weather Prediction Center (NOAA-SWPC) classifies geomagnetic storms on a 5 point “G” scale: minor, moderate, strong, severe, or extreme. The NOAA Space Weather Scales are shown in Table IX-21.

Table IX-21 NOAA Space Weather Scales

<u>Geomagnetic Storms:</u> disturbances in the geomagnetic field caused by gusts in the solar wind that blows by Earth. http://www.swpc.noaa.gov/NOAAscales/index.html#GeomagneticStorms	G1	G2	G3	G4	G5
<u>Solar Radiation Storms:</u> elevated levels of radiation that occur when the numbers of energetic particles increase. http://www.swpc.noaa.gov/NOAAscales/index.html#SolarRadiationStorms	S1	S2	S3	S4	S5
<u>Radio Blackouts:</u> disturbances of the ionosphere caused by X-ray emissions from the Sun. http://www.swpc.noaa.gov/NOAAscales/index.html#RadioBlackouts	R1	R2	R3	R4	R5

GMS Events:

- May 5, 2012: Observed a medium-strength sun storm that forecasted a G3 storm impact to Earth from May 12 through May 18. It was downgraded to a G1. Refer to the Space Weather Scales above for detailed information about the impacts at these levels.
- Halloween Storms of 2003: Space weather from these enormous solar storms slammed into Earth's magnetic field from October 19 through November 7. Aircraft had to be re-routed, it affected satellite systems and communications, and it also caused a power outage in Sweden for about an hour. The Solar and Heliospheric Observatory (SOHO) satellite, a collaboration between NASA and the European Space Agency (ESA), failed temporarily. NASA's Advanced Composition Explorer (ACE) satellite experienced damage, and instruments aboard many spacecraft had to be shut down temporarily.
- The 1859 HydroQuebec collapse was triggered by a storm of about 480 nT/min, but other storms have been measured at around 2000 nT/min (e.g., in the lower Baltic). Six million people were without power for up to nine hours that it took to bring the system back to 83 % of capacity. The 1859 storm would be in the neighborhood of 5000 nT/min. – or ten times the level of the 1859 Quebec storm. It took 17 hours for the GMS to reach Earth where it normally takes approximately 72 hours. Telegraph systems across Europe and North America failed shocking operators and igniting pylon and paper fires, stunning Aurorae was seen world-wide.

Current Situation

GIC flow concentrates in the higher voltage portions of the bulk power system. Operational procedures have been developed in many regions to increase spinning reserves, reduce demands on heavily loaded lines, and more evenly distribute the flow of power across the system in advance of a GMD. Nonetheless, recent trends are complicating the challenge including: operating the bulk power system at higher capacities with less reserve margin; building higher voltages with greater connectivity on the bulk transmission system; and the need to add more transmission capacity to accommodate intermittent wind and solar generation. As a result, the accuracy of solar weather predictions becomes more important in anticipating extreme solar events and avoiding false alarms.

Civilian space weather monitoring is primarily the responsibility of the National Oceanic and Atmospheric Administration: Space Weather Prediction Center (SWPC) in Boulder, Colorado. The SWPC can identify CME's within minutes of their appearance on the surface of the sun, but it is difficult to accurately determine whether their trajectory is directly or tangentially toward earth. Their strength and arrival time is typically within one to three days from the initial CME. Reasonably accurate forecasts are not available until the impact reaches NOAA's Advanced Composition Explorer (ACE) spacecraft, a sentinel satellite sitting about 1 million miles from Earth toward the Sun. This enables the SWPC to give a 15-30 minute warning of the likely strength of the storm. The requirement for a solar wind monitor at L1 (Lagrangian orbit number 1), a location on the Earth/ Sun line where gravitational forces can be balanced to maintain a

stable orbit, approximately 1.5 million km upstream of the Earth, would allow a 20-60 minute warning of geomagnetic disturbances at Earth (depending on velocity). This is particularly important because the ACE satellite is well beyond its operational life and while funding for a replacement has been requested for the 2012 budget, current fiscal pressures may cause it to be dropped. If ACE were to fail in the meantime, the SWPC would be unable to provide accurate near-term predictions of severe geomagnetic storms.

Power grid operators can take defensive measures to protect the grid against geomagnetic induced currents when alerted to an impending GMS by the SWPC. Monitoring incoming ground currents in real time is essential to critical grid infrastructure protection. More importantly, a number of longer-term investments could be made to reduce the vulnerabilities of the bulk power system (e.g., more robust EHV transformer designs, adding series capacitors to the system), however, such investments are expensive causing other offsetting problems (e.g., series capacitors shift currents to other parts of the system and increase demands for reactive power). Preparedness measures to protect from GMS are complex and expensive. Through the GMS Exercise, many planning opportunities were made available for future exploration and a heightened interest was evident.

Threat Description

Extreme Space Weather (ESW) is not a new problem, but the combination of ESW with a modern electric grid *IS* a new problem. http://www.ofcm.noaa.gov/swef/2012/Presentations/c-Session_3/03-02pugh.pdf

Over 746 solar-induced geomagnetic events have been measured in the past 46 years. They occur on a fairly regular basis, with only moderate or larger storms being noticed by the public due to radio or satellite interference, GPS navigation loss, or observed aurora borealis.

Fortunately no geomagnetic storms large enough to cause sustained regional power outages have been experienced since high voltage transmission power grids have been in use, the mid 1950s. None of the storms since 1950 qualify as extreme with respect to the important variation of magnetic field over time. The last large storm shown on the graph above was in February, 1942. Radar and communications were disrupted during World War II. The 1921 storm was extreme as well - impairing railroad infrastructure and radio communications.

The most notable recent severe geomagnetic storm is the Hydro Quebec power black-out of 1989. Six million people were without power for the nine hours needed to bring the system back to 83% of capacity. The Hydro Quebec collapse damaged two large step-up transformers due to over-voltage conditions. The outage was contained in the Quebec interconnection, although about 200 anomalies were felt throughout the North American bulk power system over the next 24 hours, including destruction of a large transformer at a nuclear plant in New Jersey.

Geomagnetic Storm Probability

“By virtue of their rarity, extreme space weather events, such as the Carrington Event of 1859, are difficult to study, their rates of occurrence are difficult to estimate, and prediction of a specific future event is virtually impossible. Additionally, events may be extreme relative to one parameter but normal relative to others.” (On the probability of occurrence of extreme space weather events, American Geophysical Union, SPACE WEATHER, VOL. 10, S02012, Pete Riley, Predictive Science, San Diego, USA)

Despite these challenges of extreme space weather event estimation - two researchers, Jeffery Love at United States Geological Service and Pete Riley at Predictive Sciences, have successfully produced probability calculations of a Carrington Event. Their estimation techniques and assumptions differ, but results are consistent.

Love estimates a most likely probability of one or more Carrington Events, with magnitude exceeding -1760 n/T, to be 6.3% per decade (Figure IX-44 below). Using data from, roughly the same time interval of observation - mid 1800's until current - Love estimates the probability of a megaquake (at any location on earth) to be 6.7% per decade.

In Love's estimation, the Carrington Event and megaquake probabilities are similar, as are their confidence intervals. Since risk is a function of both probability and impact, the Carrington Event provides a greater risk to society as a whole than a megaquake – given its global infrastructure effects (power, navigation, aviation, communications) versus the geographically more limited impacts of earthquakes (e.g. 2011 Tohoku earthquake).

Figure IX-44 Jeffery Love Probability Estimation Results

Anchorage, Alaska
 March 27, 1964
 Magnitude 9.2



Credible occurrence probabilities for extreme geophysical events: earthquakes, volcanic eruptions, magnetic storms
 Jeffrey J. Love, United States Geological Survey, Geomagnetism Program, Denver Colorado, USA

Poisson Event Occurrence Rates, 10-yr Occurrence Probabilities, and Corresponding Confidence-Credibility Intervals

	Since	Threshold	10-yr occurrence probability	
			Most Likely Probability of 1 or more events	Confidence Interval 95:4%
Earthquakes	1868	Magnitude = 9.5 or more	6.7%	[0.000, 0.243]
Magnetic Storms	1859	- $D_{st} = 1760$ nT or more	6.3%	[0.000, 0.230]

* $D_{st} = -1760$ nT Carrington estimate from [Lakhina et al.](#)

Note: The methodology used in Book 3A – Hazard Typology, Quick Reference Guide uses a different methodology specific to the energy sector rather than risk to the society as a whole.

Pete Riley, of Predictive Science, used an estimation technique of mathematical extrapolation from frequently observed geomagnetic storm events during the space age to derive a Carrington Event probability. Riley determined that the best data fit for observed geomagnetic storm events is a power law distribution. Extreme events thus have a more likely rate of occurrence than intuitive (e.g. normal distribution) probabilities. Riley estimates a 12% probability of a Carrington Event exceeding -850 nT per decade.

Figure IX-45 Pete Riley Probability Estimation Results

On the probability of occurrence of extreme space weather events

American Geophysical Union, SPACE WEATHER, VOL. 10, S02012
 Pete Riley, Predictive Science, San Diego, USA

- Estimation Techniques for Rare Events:
 Event Trees
 Similarity Judgments
 "Time To Event"
 → Extrapolation from Frequent Events

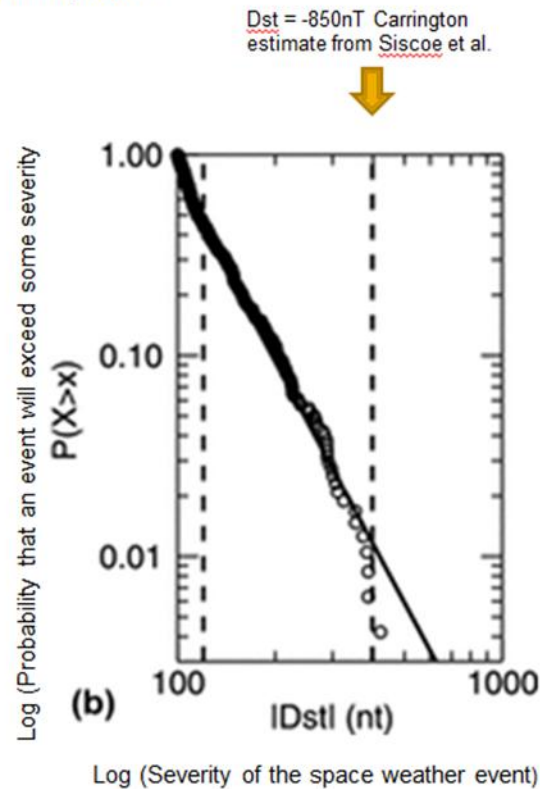
Used measured data from 746 geomagnetic storms over 46 years

Time-stationary conservative assumption:
 no solar cycle influence

Best data fit is a power law distribution

Extreme events have a higher probability than intuitive probability beliefs

12% probability of Carrington Event exceeding -850 nT per decade



Note: Pete Riley's probability estimation has similar elements as the methodology used in Book 3A – Hazard Typology, A Quick Reference Guide; however, they are not the same. The methodology used in Book 3A is specific to the energy sector.

Riley estimated a Carrington magnitude of roughly half that of Love's. His result was that the most likely probability of occurrence is double that of Love's. Results are roughly consistent between the two studies, given differing assumptions of a Carrington magnitude.

These probability estimations are useful to policy and investment decision makers in order to calibrate the risk of extreme space weather events against those of other natural disasters that are currently assessed and planned for. Geomagnetic storm risk per decade (probability and impact of extended power infrastructure damage) exceeds most other currently managed natural hazards.

Geomagnetic Storm Vulnerabilities to U.S. Power Systems

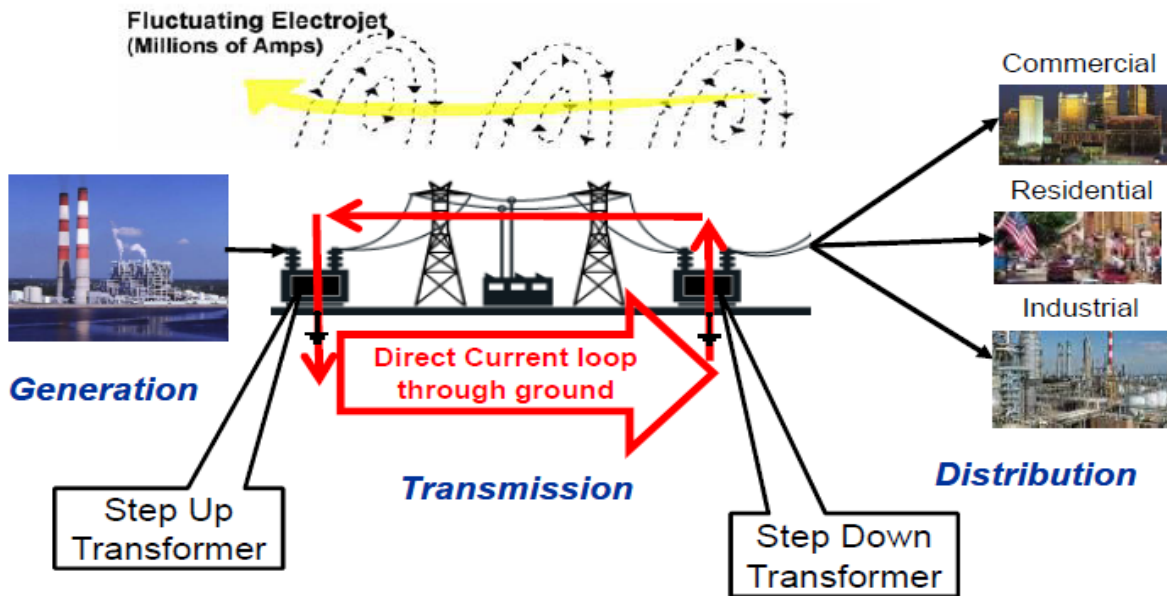
Solar magnetic storms create geomagnetic disturbances and induce ground currents, which can lead to large quasi-direct current interference in the bulk power system. System voltage collapse (due to reactive power demand) and widespread equipment failure of transformers and protective devices may result – causing prolonged blackouts or power rationing. Either failure or impairment (e.g. dielectric deterioration) of high voltage transmission assets can result in power losses that may take months or years to replace and repair. High voltage transformers are

typically custom-designed, cost several million dollars, and have manufacturing lead times of one or more years – usually from non-US manufacturers.

Many old and new (high efficiency) transformer designs used in the North American grid are susceptible to half-cycle saturation, overheating and dielectric degradation or failure – due to ground induced currents (GIC). Monitoring equipment for the detection of GIC and resulting half-cycle saturation (producing harmonic distortion) is not widely implemented in the U.S. grid. There are currently no GIC monitoring or protective (hardening) standards for the U.S. bulk power system, which is the topic of Federal Energy Regulatory Commission (FERC) Docket No. AD12-13-000, “Geomagnetic Disturbances to the Bulk Power System.” A large body of agency and industry organization studies (e.g. National Academy, NERC, IEEE, EPRI, EIS, CRO, Oak Ridge, and Homeland Security) have been published on the geomagnetic storm grid vulnerability problems and failure mechanisms in the past four years.

Figure IX-46 Geomagnetic Induced Current

Geomagnetic Induced Current (GIC) Conditions

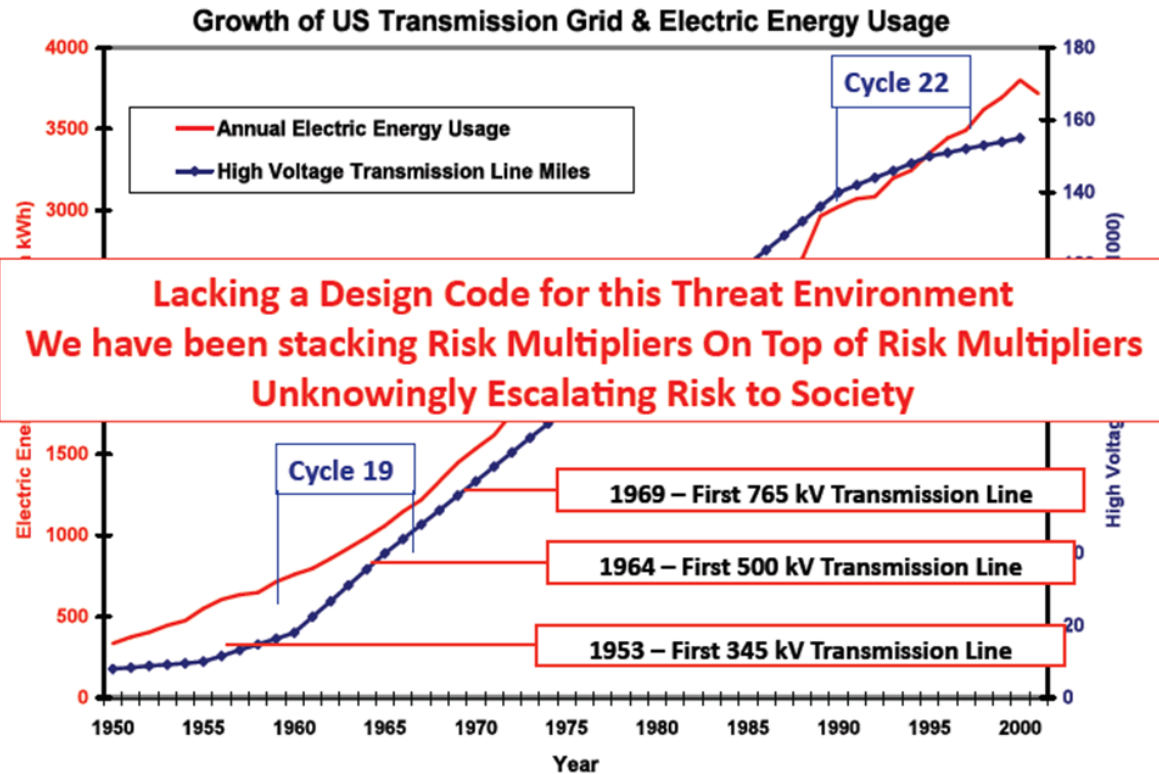


AC transformers can be damaged by DC

Source: http://www.ofcm.noaa.gov/swef/2012/Presentations/c-Session_3/03-02pugh.pdf

Figure IX-47 GIC Risk Factor

GIC Risk Factor – Growth of Transmission Network
The larger the Grid – the Larger the Antenna to cause GIC



http://event.arc.nasa.gov/sww/pdf/Kappenman_AMES_Oct16.pdf

Vulnerabilities

Grid Design Failure Criteria: A storm of this magnitude would do substantial damage to the North American grid, to include Colorado. The threat is that a GMS can develop almost instantaneously over continental-size areas. This can create “near simultaneous, correlated, multi-point failures” in the bulk power grid (Metatech-R-319 pg. 1-31). Currently the grid is designed primarily to meet n-1 failure criteria (*For multiple transmission lines delivering power to the same point, if one of the lines goes out of service, the remaining lines must be able to carry both the load they were carrying before the event, plus the load carried by the line that is out of service*) designed to manage the next worst failure after failure of the most vulnerable component on the grid. It is not designed to meet the kind of almost instantaneous failures across many parts of the system that a severe GMS could trigger.

Risk: The greatest impacts of a GMS are typically felt in higher latitudes, but are also influenced by a number of other factors, such as deep earth conductivity, which varies from region to region. More relevantly for emergency planning, the risk of damaging GIC has been substantially compounded by the expansion and increase in voltage of the bulk power grid over

recent years. The high-voltage transmission grid couples almost like an antenna through multiple ground points to the geo-electric field. Because of their higher latitudes, and more extensive and higher voltage transmission lines, the greatest risks of devastating grid damage are in the Northeast and to a somewhat lesser extent in the Northwest United States. Nonetheless, a severe storm would impact Colorado both directly as well as indirectly because of loss of ability to import power, due to outages and equipment damage throughout the North American grid.

Geomagnetic Disturbance (GMD): The primary systemic risk resulting from a severe GMD is damage to generating station and substation equipment, which then can cause cascade failures on the remainder of the system. This equipment is extremely difficult to replace. A prolonged period of time would be required to fully restore the bulk power system to normal operation. More threateningly, high GIC cause transformers to overheat and potentially suffer catastrophic failure. This is especially true of extra-high voltage (EHV) transformers. Physical damage to EHV transformers on a large scale would result in prolonged outages as they cannot be field-repaired and procurement cycles typically range from one to several years, depending on manufacturer demand. Furthermore, many components are manufactured overseas, with little manufacturing capability remaining in North America. Such an event could create a serious backlog of orders as multiple companies attempt to replace transformers simultaneously. Substation components to a lesser degree are also manufactured abroad. Unprecedented long-term energy emergency management issues would prevail.

SCADA Systems Jeopardy: A lesser focus has been on SCADA systems damage from an immediate onset of high GIC. Some observers believe this could jeopardize timely response and recovery efforts, however, SCADA systems equipment could be repaired or replaced more quickly than could EHV transformers. Thus, damage to SCADA systems would create short-term power disruption, where damage to EHV transformers and substation components would cause a long-term crisis.

Research and Analysis: The Metatech Corporation developed detailed analyses examining the potential impact of a severe GMS on the U.S. bulk power system, *Geomagnetic Storms and Their impacts on the U.S. Power Grid, January 2010*. They simulated a 4800 nT/min disturbance, which would likely saturate transformers and impose a reactive demand triggering widespread voltage collapse and a short-duration blackout. Of greater concern, their analysis indicates that the GIC would put over 350 transformers at risk of irreparable damage. Colorado would be at risk of losing 30% of its EHV transformers.

As an indication of the risk to EHV transformers, the Hydro Quebec collapse damaged two large step-up transformers due to over-voltage conditions. The outage was contained in the Quebec interconnection, although about 200 anomalies were felt throughout the North American bulk power system over the next 24 hours as the storm extended south into the U.S., including damage to a large transformer at a nuclear plant in New Jersey.

A more recent storm caused a regional blackout in Sweden in October 2003 and caused permanent loss of 15 EHV transformers in the Eskom system in South Africa.

Interdependencies: Increasing dependence on natural gas instead of coal for generation could quickly impact power availability, though it appears that the natural gas distribution system is more resilient in the face of power disruption than vice versa.

- New Mexico rolling blackout in early 2011 when gas lines froze
- Economic indications: The need for quick ramp rates to balance fluctuating wind and solar
- Loss of power will impact ability to pump liquid fuels requiring back-up power generation
 - Limited on-site supply
 - Database of State assets with/without back-up power generation does not exist
 - Almost no fuels storage capacity for State facilities
- Loss of power affects virtually every critical infrastructure sector

<ul style="list-style-type: none"> – Energy – Emergency Services – Government Facilities – Dams – Water – Food and Agriculture – Banking and Finance – Information Technology – Communications 	<ul style="list-style-type: none"> – Transportation Systems – Healthcare/Public Health – Defense – Commercial Facilities – Postal and Shipping – Critical Manufacturing – Chemical – Nuclear Reactors – National Monuments and Icons
---	---

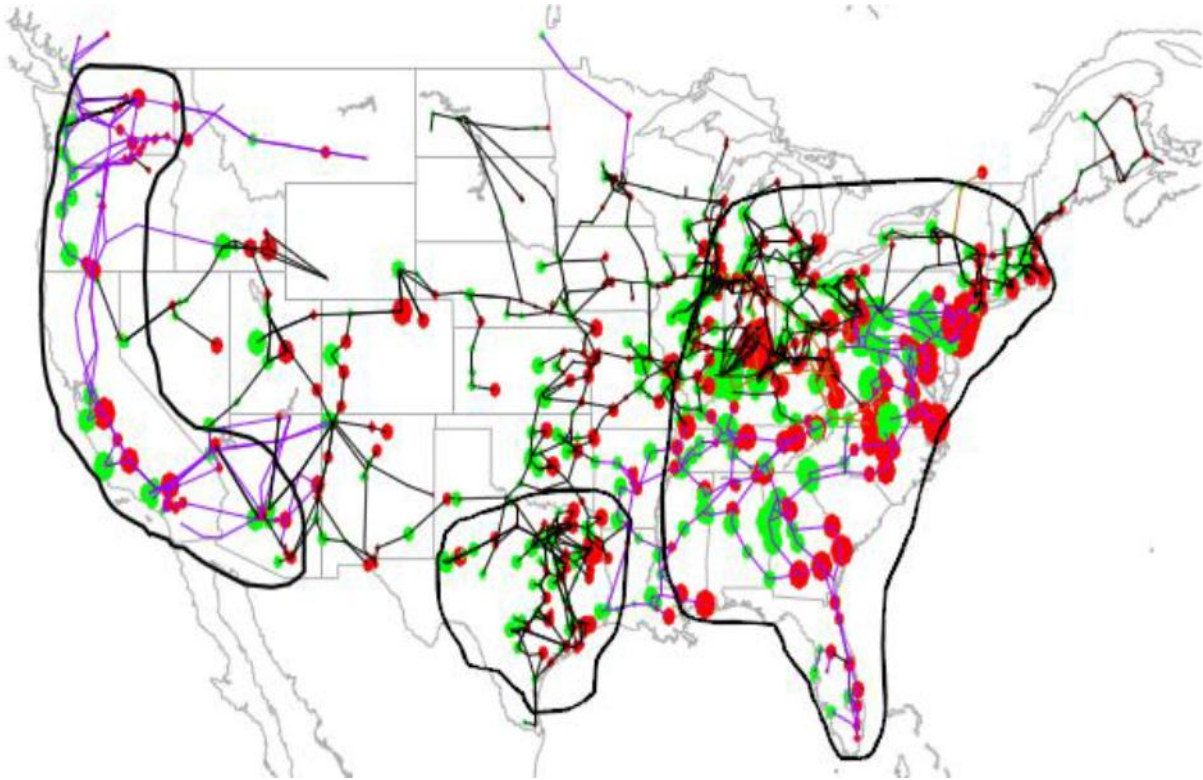
Potential Costs

An estimate of \$1 to \$2 trillion during the first year alone was given for the societal and economic costs of a “severe geomagnetic storm scenario,” with recovery times of 4 to 10 years (National Academy of Sciences). Economic cost of the August 2003 Northeast blackout was \$4 -10 billion.

Colorado Risk of GMS

Colorado power is supplied through both high voltage connections within the state and to adjacent states. (Figure IX-48) An estimated 30% of EVH transformers used in Colorado may be at risk of permanent loss or damage in an extreme geophysical storm - as presented at the October, 2011 NASA Ames Research, “Space Weather Risks and Society Workshop” (second graphic following). The Rocky Mountain region was one of the most disturbed geomagnetic field environments during the geomagnetic storm of March 13-14, 1989 (third graphic following).

Figure IX-48 High Voltage Connections

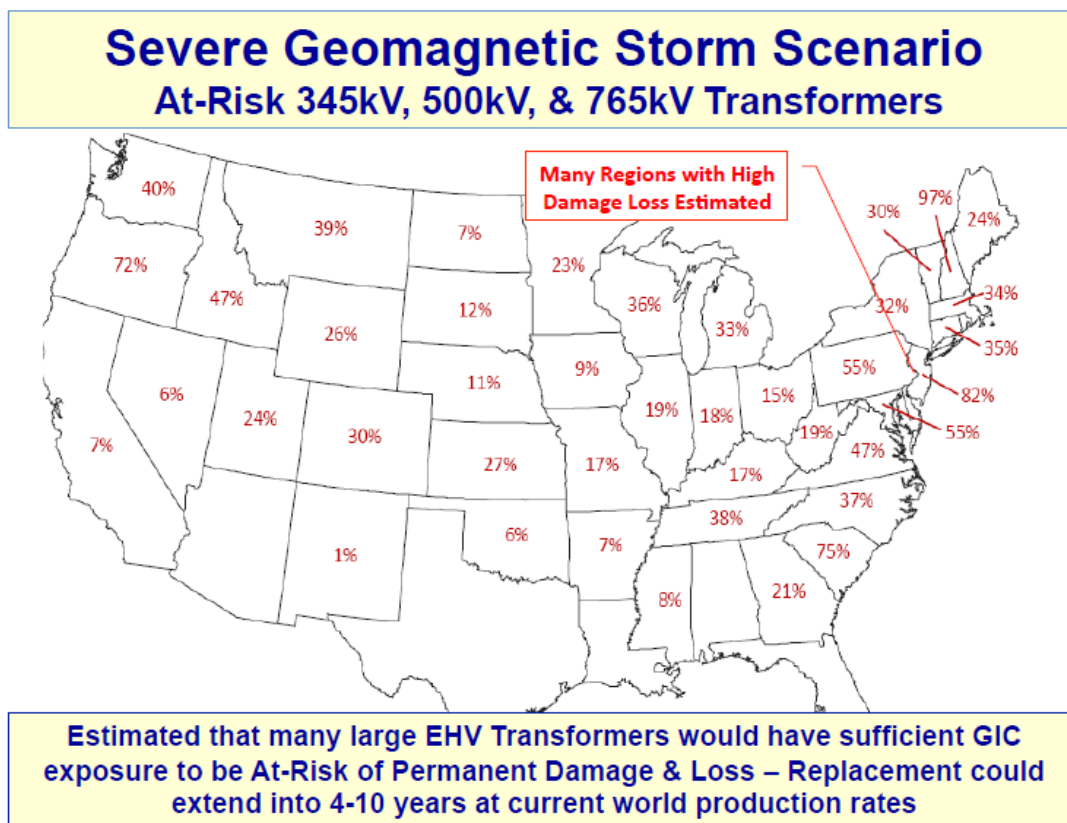


Source: Metatech Corporation for Oak Ridge National Laboratory, "Geomagnetic Storms and Their Impacts on the U.S. Power Grid," 2010

Scenario: 45 Degree Electrojet over East Coast

The above regions outlined are susceptible to system collapse due to the effects of the GIC disturbance in a "100 year" geomagnetic storm. The black lines indicate extra-high-voltage transmission lines and major substations. The red dots indicate the locations and magnitude of the geomagnetically induced currents that would flow across the network.

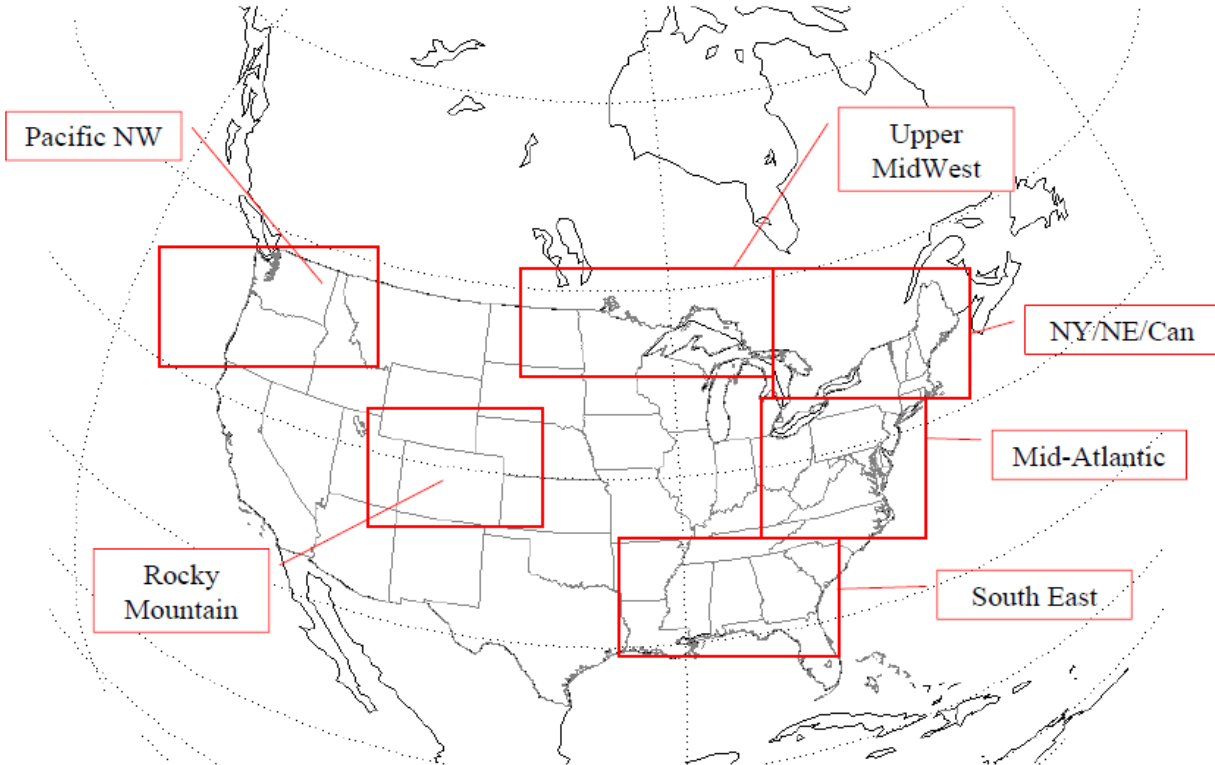
Figure IX-49 At-Risk Transformers



Note: Colorado has one of the highest percentage estimates of at-risk EHV transformer assets in the Western United States.
http://event.arc.nasa.gov/sws/pdf/Kappenman_AMES_Oct16.pdf

Colorado was one of the most disturbed geomagnetic field environments on March 13-14, 1989.

Figure IX-50 GMS Impacts on U.S. Power Grid



Source: Metatech Corporation for Oak Ridge National Laboratory, "Geomagnetic Storms and Their Impacts on the U.S. Power Grid," 2010. <http://www.fas.org/irp/eprint/geomag.pdf>

Power Grid Outages by GMS

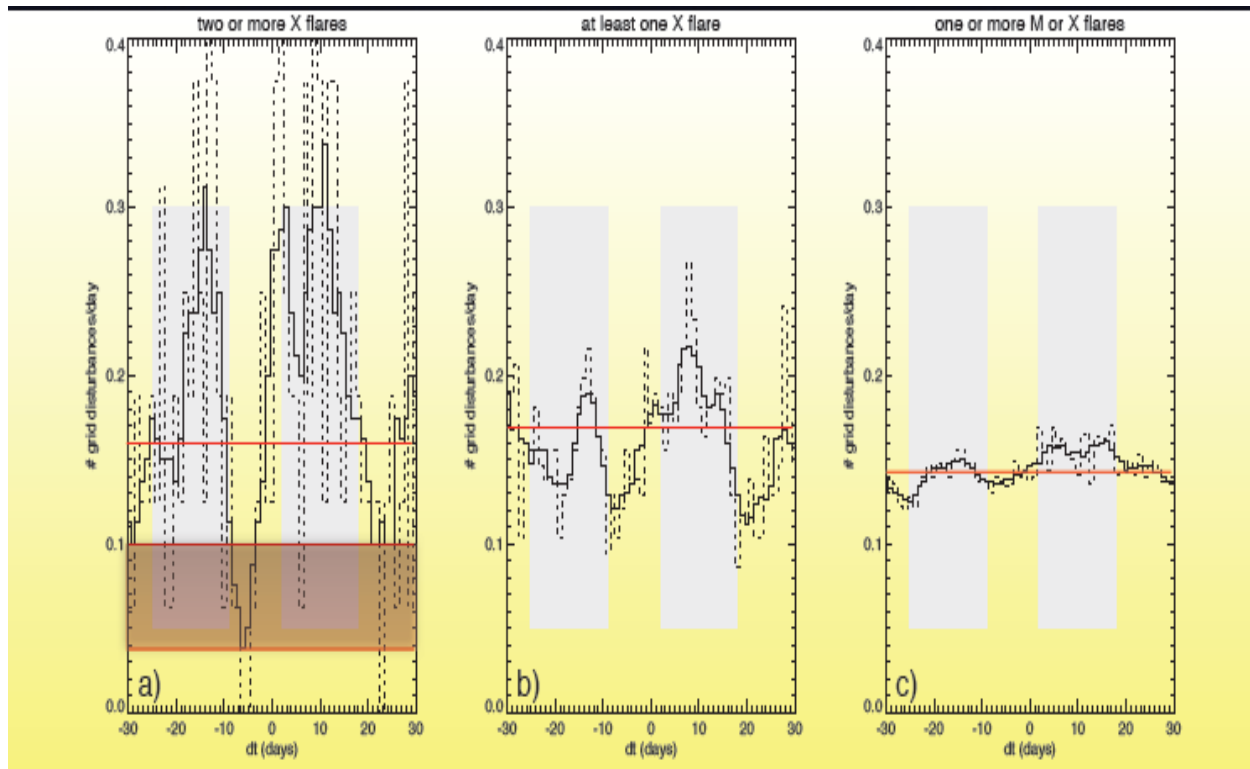
Lockheed Martin Advanced Technology has correlated a large number of solar event measurements with documented (NERC and DOE data) North American power outages during a 19 year study period. Their new research publication is in review as of June 2012. Published in the NERC-DOE power outage reports over the 19 year period studied (1992 through 2010), no outages were attributed to solar weather as a primary or contributing cause of power outages.

"This is to be contrasted to our finding that ~60 grid disturbances large enough to require reporting to DOE and NERC should be attributable to major solar flares, with at least another ~60 cases related to other space weather around the time of major flaring over that same period." (Karel Schrijver, Sarah Mitchell, Lockheed Martin Advanced Technology Center, "Space Weather: what does it cost and how bad can it get?" Space Weather Enterprise Forum, 2012)

"Non-catastrophic disturbances in the US power grid (reported to and by NERC & DOE) occur regularly subject to "normal" space-weather conditions: ..."

"The average cost to the U.S. economy of grid disturbances attributable – *but not officially attributed* – to relatively common solar activity is as high as \$4 billion." (Schrijver and Mitchell, 2012, subm.)

Figure IX-51 Grid Disturbances Daily Count



Source: http://science.nasa.gov/media/medialibrary/2012/03/01/Schrijver_HPS20120228_SSW201202.pdf

The correlation of grid disturbances with major solar flaring reveals a weakness in the US power grid not recognized. Dotted histogram: Daily count of grid disturbances. Solid histogram: 5-day running average of grid disturbances. Red line: Zero line – disturbances 1 day before flare occurs. Gray boxes: the period of enhanced grid disturbance frequency.

GMS Risk Mitigation: Warning and Planning. Grid Monitoring.

The NOAA Space Weather Prediction Center (SWPC) in Boulder, CO provides a valuable space weather warning service to power grid operators, aviation, satellite operators, communications and other critical users, but an early warning system that can be used to prevent grid asset damage does not yet exist.

Ideally, a space weather warning system could be used by power system operators to take protective measures for critical assets in the event of an incoming extreme geomagnetic storm event.

NOAA Space Weather solar observations are made using multiple terrestrial telescopic and satellite platforms. “Fast transit” CME events (such as the Carrington Event) take between 15 and 22 hours in transit between the sun and earth. The ACE satellite (launched 1997 for a six year life) is the only current satellite asset that can measure incoming magnitudes and

polarization of severe space weather events – less than 30 minutes before a “fast transit” impact with the earth’s magnetosphere.

Even if this very short measurement and warning interval could be managed by power system operators, there are two major problems with current predictive capabilities: survivability and false positives/ missed positives. Regarding survivability, there is doubt that the ACE satellite would survive the initial storm of energetic particles in an extreme CME event.

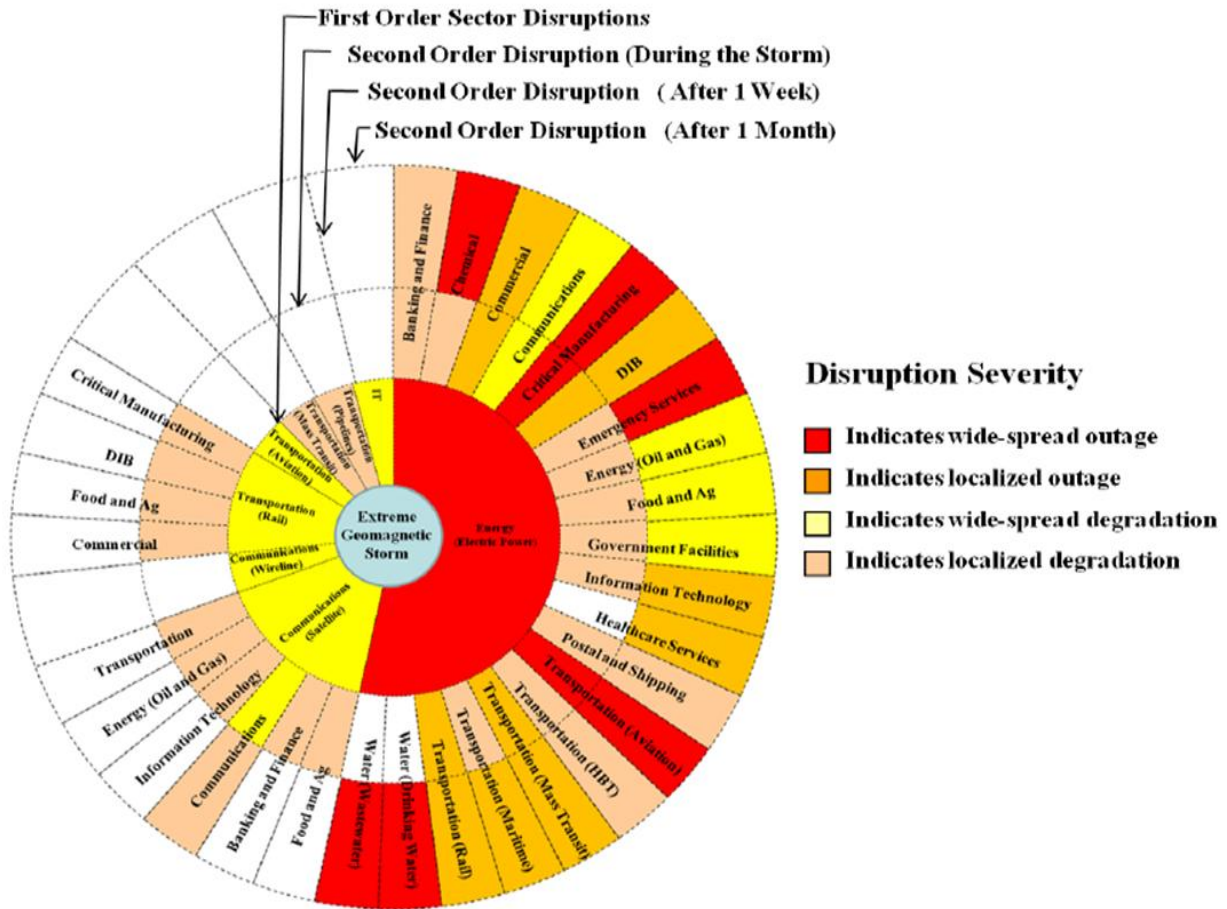
The best geomagnetic storm detection model tested produces over 20% false positives and misses 20% of true positives. This error rate would be difficult to use in making a critical decision to force network black-outs or shut-downs. Such actions could produce network instability, economic damage and potential loss of life – from human produced black-outs.

New satellite assets and improvements in detection and estimation modeling science are needed (and have been proposed) in order to create a reliably accurate grid asset protection mechanism from space weather observations. The current NOAA operational warning capabilities are valuable to grid operators only as a “stand-up” and “stand-down” warning system – to alert personnel and operating practices (e.g. maintenance) to the potential of a moderate, strong, severe or extreme space weather event. Reliable and actionable prediction of geomagnetic storm event incidence is currently beyond our scientific and investment maturity. Although substantial research progress is being made by multiple groups and agencies, a decision for national investment has not yet been made.

Mitigating Grid Asset Failures

A viable, actionable protective solution today would be to monitor grid assets for early failure indications (e.g. sudden reactive power demand, GIC currents, and harmonics), and take early corrective actions (including disconnects and generation shut-down procedures). Transformer asset protection response times needed are believed to be within 10 seconds – requiring automation instead of human decision making. Unfortunately, these capabilities are not required, standardized, nor widely implemented in the U.S. power grid. This is both a public policy and investment decision regarding power system security that has yet to be made.

Figure IX-52 Power Interdependencies with Other Critical Infrastructures



Source: OECD/IFP Futures Project on Future Global Shocks, “Geomagnetic Storms,” CENTRA Technology, Inc., on behalf of Office of Risk Management and Analysis, United States Department of Homeland Security, 2011. <http://www.oecd.org/dataoecd/57/25/46891645.pdf>

This infrastructure interdependency illustration diagrams “that the severity of disruptions to different critical infrastructures selectively worsens over time. Some sectors are able to maintain continuous operations for a short period of time, such as drinking water or health care facilities. Even these, however, begin to see degradation of services after a week without power. If the power outage continues for over a month, then critical outages emerge in sectors that have public safety implications, such as drinking water, wastewater, emergency services, and health care. Note that these cascading effects are possible, but depend on the specifics of the affected areas.”

GMS Event Management Planning

The establishment of North American geomagnetic storm grid hardening standards will most likely lead to many years of monitoring/control and equipment and network upgrade investments to the North American bulk power system. The regulatory process has just begun (May 2012) of determining if GMD protective standards should be established, and what the nature and

priorities of those standards should be, which is the topic of FERC Docket No. AD12-13-000, “Geomagnetic Disturbances to the Bulk Power System.”

Waiting to see if the U.S. bulk power systems will be improved or hardened over time is not a prudent option for emergency management planning in the state of Colorado. The risk of geomagnetic storm damage or impairment to Colorado power availability is immediate and ongoing. One or more extreme space weather events (Carrington equivalent) are estimated at between 6% and 12% per decade by researchers at USGS and Predictive Science, respectively.

FEMA has stated publicly that managing a wide-scale, long-term outage of the bulk power system is beyond the scope of their resources and encourage regional and local plans.

A prudent immediate solution to consider could be to protect the economic livelihood and safety of Colorado citizens through planning for state and regional emergency power rationing, in coordination with WECC and utility operators serving the state. Critical power users need to be identified, prioritized and incorporated into the plan. Emergency management services, hospitals, transportation fuel, gas, water and sanitation are some of the critical power users that should be reviewed and prioritized.

The resulting Colorado power restoration and allocation plan should be communicated and agreed upon between all stakeholders. The plan should include the following components:

- Discovery of proprietary utility customer contracts
- Discovery of vulnerable transmission links (At-risk EHV transformer estimation)
- Participation of the PUC
- Clarify Roles and Authorities
- Assess Risks
- Conduct Technical Studies
- Prioritize Assets
- Identify Interdependencies
- Evaluate and Test
- Develop and Promote Guidelines
- Communicate Funding Needs

Potential Mitigation Initiatives

A number of protocols were suggested by NERC to reduce the risks of GMS and electromagnetic pulse (EMP), a high altitude nuclear detonation, which would have similar effects as geomagnetic disturbances. They include:

- Create a task force of industry, equipment manufacturers, and risk experts to identify a cost-effective “top ten” mitigation list
- Pursue continued support from government authorities

- Develop a long-term research roadmap
- Develop advanced methods to ensure that operators are given region-specific, timely, and accurate information regarding the expected duration, intensity and geographic footprint of impending GMDs
- Develop an alert procedure to inform the electric sector of threat levels

Since the study, NERC has developed a working-relationship with the SWPC and a GMS working group of major utilities are attempting to better quantify the risks and to clarify the likely effectiveness of preventative steps. Limited manufacturing capacity for transformers exists in North America requiring offshore procurement with delivery time up to 24 months. The “Spare Transformer Equipment Program” (STEP) run by the Edison Electric Institute and the Department of Homeland Security Science & Technology Directorate Recovery Transformer Project, are important initiatives where ongoing efforts to improve these programs should continue. With respect to the entire grid, remedial measures to reduce GIC levels are needed and cost-effective. The installation of supplemental transformer neutral ground resistors to reduce GIC flows is relatively inexpensive, has low engineering tradeoffs, and can produce 60-70 percent reductions in GIC levels for storms of all sizes. Installation of series capacitors can also be a cost-effective remedy for reducing GIC. The Eastern grid has very few series compensators where the Western grid has substantially more, but none in Colorado.

Other HILP Events

This section only focuses on Cyber Warfare and Solar Weather as these HILP events were deemed as most likely to occur given the background information and scientific data. There are many other types of High Impact/Low Probability Events that are not extensively detailed in this section. In Book 3A, Hazard Typology, other such events including large-scale Earthquakes and human-caused hazards to include Chemical, Biological, Explosive, Radiological, and Nuclear are discussed and rated through a methodological process that determines a likely probability for impact to the energy sector from such an event.

Recommendations

- Establish Pros and Cons for a “black start” scenario protocol for system restoration when all generation is completely shut down and a significant number of assets face some degree of physical damage.
- Encourage major systems operators develop protocol for operating in a conservative state should a major GMD event be expected. Conduct exercises and drills.
- Continued research through the Electric Power Research Institute
- Monitor EPRI’s SUNBURST publication
- Consider the antenna effect when adding transmission to the bulk power system.
- Potential concern when adding long transmission lines to bring remote wind or solar power to main Colorado load centers

- “Grid Reliability” and Infrastructure Defense Act (HR 5026) passed the House, but not the Senate: continue to monitor grid reliability legislation
- Develop a High Impact/Low Probability Events Framework
http://www.sintef.no/project/Vulnerability%20and%20security/Publications/Papers/0094_Framework%20HILP_CIREd-WS_Lyon2010.pdf

Exercises

Introduction

Scenario-based exercises offer the exercise design team and participating jurisdiction officials the opportunity to evaluate the efficiency of processes in place that would be implemented during an emergency or disaster. Exercises mock an actual threat or hazard that may be characteristic to a specific jurisdiction or to better understand potential impacts from unexpected or unusual disaster events, such as High Impact/Low Probability (HILP) events, like the attack on the World Trade Center on 9/11. The distinction between HILP and other disaster events is the basis of predictability and probability that an event will occur. Hurricane Katrina was certainly high impact, but it was not only predictable but probable three days in advance. A large scale cyber attack might be probable, but may not be predictable. On the other hand, a geomagnetic storm event is only predictable if a solar flare is detected and only probable if it is in a direct path toward Earth. True HILP events have an incredibly short impact time frame without the luxury of pro-active response where decision-making is significantly different than in non-HILP events.

Each State receiving EA funding was required to conduct two exercises; 1) an **Intra-State** exercise, and 2) an **Inter-State** exercise or could participate in a Regional exercise orchestrated by the U.S. Department of Energy (DOE) and the National Association of State Energy Officials (NASEO) to satisfy the requirement for an Inter-State exercise. Colorado chose to conduct an intra and inter-State exercise and participate in the DOE Regional exercise. Ten members representing local and State government, private utilities, and private EA contractors participated in the Western Region Energy Assurance Exercise, in Phoenix, AZ in November 2011. The goal of all exercises was to explore and improve the overall command, control and communications between primary energy stakeholders and local, State and Federal agencies during an energy emergency or crisis. The details of each exercise are discussed in detail below with an overall synopsis of the outcome as the summary. The After Action Reports (AARs) can be reviewed in full in the appendices.

Organization

Exercises are facilitated to expose gaps and vulnerabilities in preparedness and response plans with the intent to implement corrective actions to mitigate or close gaps identified. The exercise design team formed from members of the Energy Assurance Advisory Group (EAAG) set objectives then built the scenarios to meet those objectives. A cyber attack scenario with impact on electric utility network infrastructure was agreed upon for the Intra-State exercise, and a geomagnetic storm scenario with impact to regional critical infrastructure was agreed upon for the Inter-State exercise. Each exercise followed the Homeland Security Exercise and Evaluation Program (HSEEP) methodology to ensure compliance with the Department of Homeland Security and the Division of Emergency Management exercise and training procedures.

The exercises were conducted during the EA planning process as opposed to after the EA planning process to correlate and focus on specific workshop content and learn about existing processes during an energy emergency from a well-represented cross-sector group. Significant emphasis was placed on ensuring that the stakeholders with an active role in a real-time event would be available for participation. The duration of each exercise was approximately five hours to include time for a “hot wash” at the close of the exercise. The exercise itself was facilitated by the EA Exercise Coordinator, who presented a series of realistic occurrences to stimulate discussion relative to actual response actions that would be taken by each participating stakeholder in an actual event. The exercises afforded the opportunity for participants to comprehend the complexity of electric grid impacts and cascade systems failure due to the interdependencies of all other sectors on the energy sector. Understanding the capability gaps exposed from facilitating these exercises was instrumental in the development of the Goals, Potential *Initiatives*, and *Potential Action Items* of the Plan itself.

Intra/Inter-State Exercise: Cyber Attack

Scenario: Cyber Attack

Conducted Wednesday June 29th, 2011, hosted by the Jefferson County Sheriff’s Office

Intra/Inter-State Exercise – Cyber Attack

Participants and Stakeholders in Attendance

AMEC Earth and Environmental, Inc.....	Jeff Brislaw Hilary King
Battelle	Mike Spender
City of Aurora	Matt Chapman Karen Hancock Porter Ingrum Marena Latch
City of Fort Collins	Wayne Sterler
City of Lakewood represented by EA Contractor SAIC	Sabine Bendanoun
Colorado Solar Volts.....	Marvin Owens
Colorado Springs Utilities.....	K. Kirshna Tama Wagoner
Colorado Division of Emergency Management	Kerry Kimble Jason Finehout
Colorado Department of Regulatory Agencies – Public Utilities Commission	Larry Duran
Colorado Energy Office	Matt Futch

Introduction

The Intra-State exercise included Regional participation, thus qualified for both state and inter-state collaboration. It was a discussion-based, no fault table-top exercise. This exercise was scheduled directly following Workshop #3 – Cyber Security. Workshop #3 offered distinguished speakers from the Department of Energy (DOE) and the National Institute of Standards and Technology (NIST) presenting information on Cyber Security Standards and the Smart Grid Interoperability Panel and Priority Action Plans to a well-attended audience of interested stakeholders from local, State, and Federal agencies, as well as representatives from public and private utility organizations, and other associated participants. The cyber Exercise Design Team was identified at this workshop and participated in developing the details of the cyber attack scenario presented here. A number of cyber injects were developed to simulate that the occurrences had taken place over a number of months. Each inject was expanded upon in the subsequent inject presenting a scenario of cascading failure on utility infrastructure. The EA Exercise Coordinator collected comments, suggestions, concerns and recommendations throughout the exercise and the following hot-wash. The following sub-section describes the current environment of vulnerability within existing networks and the exponential risk of systems failure through cyber attack as global communication and social networks expand. It is with this understanding that the Exercise Design Team decided a cyber attack would be the most appropriate scenario for the Intra-State Exercise.

Understanding the Smart Grid and Cyber Security

Although Cyber Warfare is discussed in detail in the previous HILP Events section, the following information is focused on the application of Smart Grid technologies to the current Grid and the potential impacts from cyber invasion on an improved grid system.

Many utilities across Colorado are taking steps to modernize their power infrastructure in an attempt to manage peak demand, improve system performance, and improve energy efficiency. Like multiple utilities across the U.S., Colorado's utilities are in various stages of deploying an overlay of bi-directional, real-time digital communications networks and highly automated digital control networks. This combination of advanced Information and Communications Technology (ICT) with traditional electricity operational infrastructure enables the transformation commonly known as "Smart Grid".

The Smart Grid will apply interconnected elements that optimize communications and control across the different segments of energy generation, distribution, and consumption. A properly designed Smart Grid infrastructure is intended to enable utilities to manage their entire electricity system as an integrated framework, actively sensing and responding to changes in power demand, supply, costs, quality, and emissions across various locations and devices. A Smart Grid is also intended to extend grid connectivity to customer-owned distributed generation technologies, such as solar panels, wind turbines and plug-in hybrid electric vehicles (PHEV). Future smart grid applications may also include key roles for energy storage, in particular,

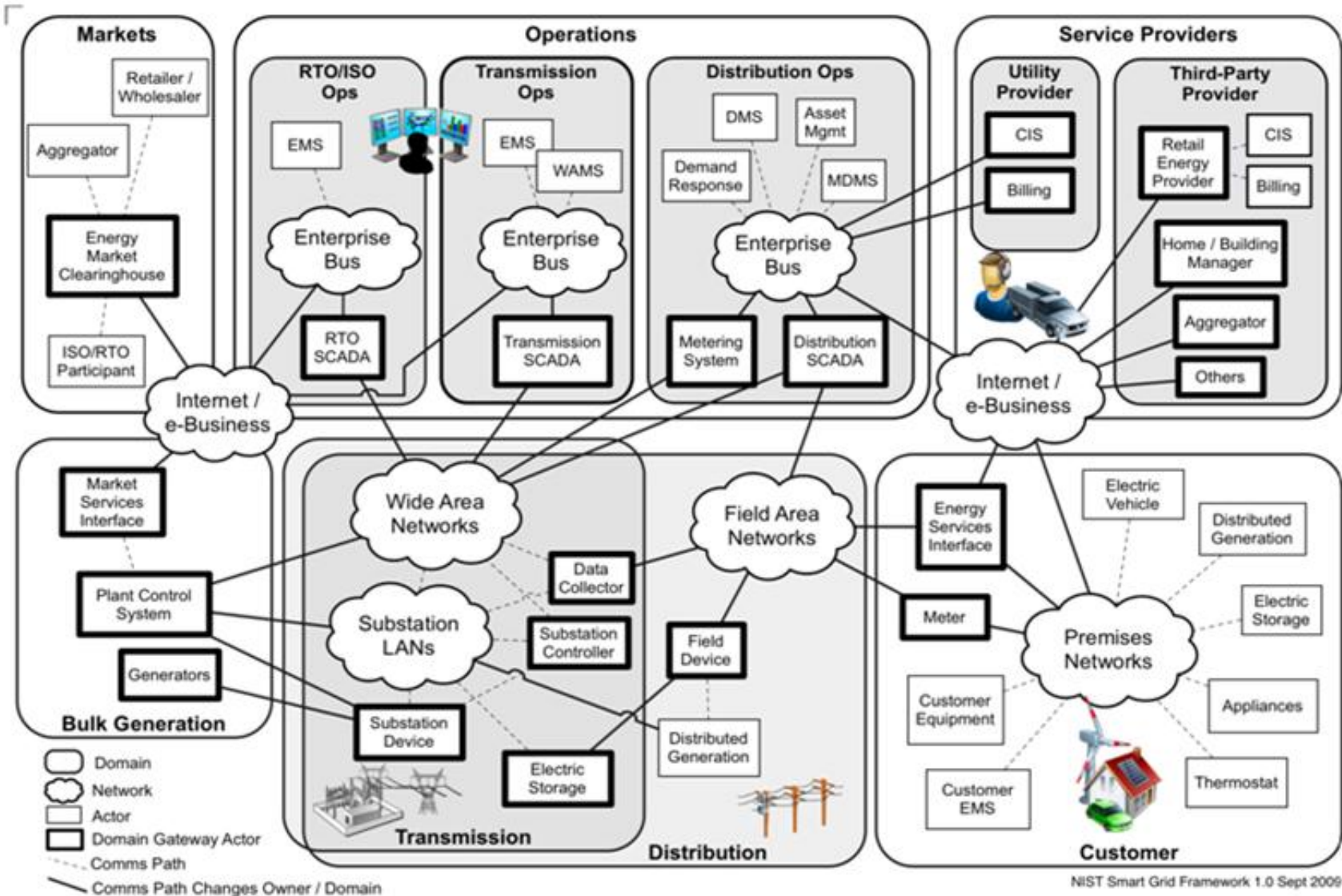
storing electricity that is generated when it is inexpensive to produce. This may involve using improved battery technology, including the batteries in PHEV's. The National Institute of Standards, an agency of the U.S. Commerce Department, identified seven major domains within a smart grid: Markets, Operations, Service Providers, Bulk Generation, Transmission, Distribution, and Customers, as displayed in Figure IX-53.

Funding appropriations in the American Recovery and Reinvestment Act have stimulated increased deployment of smart grid technologies and applications. Many of these components are critical to interoperability and reliability, will communicate bi-directionally, and will be tasked with maintaining Confidentiality, Integrity, and Availability (CIA) vital to power systems operation. This extension of two-way digital technology to electricity infrastructure shows much promise for utilities to improve operational efficiency, to reduce costs, and to integrate renewable sources of energy. The flip side is that the deployment of numerous additional ICT nodes and "smart" devices connecting utilities to their customers introduces a high degree of vulnerability to cyber events (whether accidental or malicious in origin) and provides new openings for intruders. The interconnected, crosscutting and horizontal nature of networked technology provides the means for an intelligent cyber attacker to impact multiple assets at once, and from anywhere.

The inclusion of "smart phones" into the smart grid, distribution automation and distributed generation equation represents another alarming vulnerability to utilities. While more than 1.5 billion people use the internet each day, over 4.5 billion uses a cell phone. An estimated 2 billion "smart phones", are estimated to be deployed by 2013, with an ever-rising number of applications available that enable even rural dwellers to access the internet. As internet-based energy management system (EMS) application is modified for "smart phone" devices, they provide an alarming volume of vulnerable entry points for cyber intrusion.

A Smart Grid domain is a high-level grouping of organizations, buildings, individuals, systems, devices, or other *actors* with similar objectives and relying on—or participating in—similar types of applications. The various actors are needed to transmit, store, edit, and process the information needed within the Smart Grid.

Figure IX-53 The domains in the NIST logical reference model include Markets, Operations, Service Providers, Bulk Generation, Transmission, Distribution, and Customers.



The critical role of cyber security in ensuring the effective operation of the Smart Grid is documented in legislation and in the Department of Energy's *Energy Sector Plan*. Section 1301 of the Energy Independence and Security Act of 2007 (P.L. 110-140) states:

It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth and to achieve each of the following, which together characterize a Smart Grid:

- 1) Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid*
- 2) Dynamic optimization of grid operations and resources, with full cyber-security*

Despite the legislative focus on cyber security, the rush to deploy millions of "smart" devices is often carried out without due consideration of security risks. A 2010 Center for Strategic and International Studies (CSIS) survey of utility executives found that nearly a third indicated that their sector was either "not at all prepared" or "not very prepared" to deal with attacks or infiltration by high-level adversaries. Among those who had actually experienced such attacks, this lack of confidence rises to 41 percent.

Many cyber security experts point to a lack of security features being built into utility smart grid systems. A report from Ponemon Institute found that only 29 percent of surveyed executives at utility and energy companies fully understood and appreciated the need for security. The report found that most utility and energy companies focused security efforts on minimizing downtime and complying with regulatory and legal requirements. Only 5 percent of respondents reported that preventing or minimizing advanced persistent threats was a top security goal. Major utilities in Colorado reveal that cyber security preventive measures in new projects are often left off the budget as they can prevent or delay the approval process or allow projects to meet marketing imposed implementation deadlines.

Utilities across the U.S. reporting cyber attacks are alarmed at the increase. A U.S. Government Accounting Office analysis based upon Carnegie Mellon University's Computer Emergency Response Team (CERT) Coordination Center data reveals that seventy percent of energy and power companies experienced some kind of severe cyber attack on their Information Technology or Supervisory Control and Data Acquisition (SCADA) / Energy Management System (EMS) network. A survey of companies responsible for critical infrastructure conducted by the Center for Strategic and International Studies (CSIS) found that two thirds of respondents reported that cyber attacks had harmed company operations. Eighty percent of the executives reported large-scale denial-of-service (DOS) attacks. The issue of cyber security took on ever greater importance following the Stuxnet worm that disabled nuclear reactors in Iran. Nearly seventy percent of the CSIS survey report frequently finding malware designed to sabotage their systems,

and nearly fifty percent of electric utility executives reported having found Stuxnet in their systems

In this November 2010 testimony before the United States Senate Committee on Homeland Security the ex-chief security officer for the North American Electric Reliability Corporation (NERC) and current Chief Executive Officer of the National Board of Information Security Examiners for the United States, provided a sobering assessment of cyber defense within the energy industry:

"Current defense and protection models are not sufficient against highly-structured and resourced cyber adversaries capable of employing new and high-consequence attacks. We must develop and implement protection strategies that accept the unfortunate, though probable, reality that many of our networks are already contested territory. This requires a shift of our priorities from a prevention-heavy approach to reduce the likelihood of such an event from occurring to a greater focus on minimizing the possible consequences of such an event"

Cyber security needs to be appropriately applied to the combined power system and IT communication system domains to maintain the reliability of the Smart Grid and privacy of consumer information. Cyber security in the Smart Grid must include a balance of both power and cyber system technologies and processes in IT and power system operations and governance. At the same time, cyber security measures in these systems must not impede safe, reliable power system operations.

For more information on the vulnerabilities and mitigation strategies related to cyber invasion events, please see Section VII – High Impact/Low Probability (HILP) Hazard Events.

Exercise Elements

Exercise Design Team

Members of the Exercise Design Team for the Intra-State exercise represented the following organizations: Xcel Energy, Black Hills Corporation, Colorado Energy Office, City of Fort Collins, City of Aurora, Division of Emergency Management, DORA – Public Utilities Commission, Batelle, Northcom, and EA contractor – CISPR, LLC.

Setting

The exercise setting was established by depicting the current national environment. Current events of domestic and foreign political tension, financial crisis, natural disaster, and sports news were presented. An introduction to the utilities environment was also presented, which further set the stage for a better understanding of utilities' operations on a daily, monthly and yearly basis as they handle weather events, grid maintenance, regulations, and major outages. As part of the pre-event stage, a number of best practices for 'Cyber Hygiene' were discussed. Cyber Hygiene involves activities and protections that should be in place to minimally shield the ever evolving, dodging threat of cyber attack. This process is also referred to in the security industry as "defense in depth."

Risk and vulnerability of Supervisory Control and Data Acquisition (SCADA) environments, which refers to the industrial control systems that monitor and control industrial infrastructure or facility-based processes, were also discussed, involving a number of information technologies implemented around SCADA environments; and that a growing community of software engineers is able to exploit the vulnerabilities of SCADA and IT systems increasing risk.

Objectives

The objectives of the Cyber exercise were to explore the preparation, protections, response and recovery from a cyber attack on utilities critical infrastructure.

- Explore threats and hazards to utilities
- Discuss potential vulnerabilities
 - SCADA vs. IT systems
 - Smart Meters or AMI
- Explore defenses
 - Cyber Hygiene
 - Generation, Transmission and Distribution diversity
 - Large number of entities involved in Colorado
- Explore implications of Smart Grid technologies
- Explore implications of renewable technologies
- Look for opportunities/methods to share threat information

Scenario

A Phishing scam was presented as the first scenario inject, leading to a botnet, which is a collection of compromised computers where code commands the group to be controlled by the infiltrator. Expanding on the Phishing attack, a second inject was introduced known as an Advanced Persistent Threat, which is characterized as a group with the capability and intent to persistently and efficiently target a specific entity. This simulated that the invader was capable of altering attack methods by monitoring the changes in defense tactics. Discussions followed each inject. Based on discussions of impacts that would be experienced in this scenario, damage to utility infrastructure, generation, and equipment would be inevitable. Specific cyber security protection measures among stakeholder agencies were considered proprietary and were not discussed. Although all participants were in agreement that a Cyber Security Working Group would be in order to advance protection for interconnecting networks.

Exercise Results

Strengths

- An informal network among utilities cyber and IT staff for information sharing exists
- A one-hour reporting requirement exists for utilities to report a major penetration.
 - Reference DOE OE 417
 - There are 10 criteria that require reporting within 10 hours
 - Others require reporting within one to six hours
- Information Security product vendors do form a pseudo information sharing environment when they serve multiple customers in the same sector, in this case utilities.
- PUC supports recommended standards from FERC/NIST and NERC.

Capability Gaps

- No formal information sharing network between the utilities and State or Federal agencies exist
- DEM does not receive reports on cyber attacks that may be the cause of current or potential outages.

Noted Issues

- Reporting authority question: “If utilities are the victim of an attack, who should they report to?”
 - Depends on severity and impact
 - Cyber attack with no impact on delivery or services
 - Cyber Attack, or any other impact, that impact service delivery
 - When and how would DEM, CEO, PUC, and Federal agencies receive the report?
- Utilities implementing Smart Grid technologies collect and use significant amounts of customer usage data that could be used by criminal elements to track residential and business customer patterns or personal behavior patterns
- Cyber security preventive measures in new projects are often left off the budget as they can prevent or delay the approval process or allow projects to meet marketing imposed implementation deadlines
- Phishing, human/social engineering attacks, are likely infiltration points than manufacturer introduced malware. This is especially true during a high stress or emergency situation when security protocols could be inadvertently relaxed or compromised to get back to business as usual
- Utilities are comfortable with sharing information with State and Federal regulators, however, uncomfortable that information could get into the hands of media and the public, given the level of expectations and the rapid speed of dissemination through social and media networks, the potential to misunderstand the information or use the information inappropriately would create a bad public perception of the utility
- What responsibilities do information security vendors have when they are trying to resolve issues with customers while simultaneously marketing their security products and expertise in resolving issues?

Areas of Concern

(Indicates further examination required for potential solutions to be developed)

- Need the ability to notify cyber defense / counter intelligence services when an attack occurs so that patterns can be developed
- Utilities should provide cyber security protections as part of any new project that implements or changes IT, communications networks or SCADA technology
- The Industry, along with State and Federal regulators, should engage in setting guidelines with flexibility in how they are implemented
- Public perceptions of power outages should be re-stated. A 72 hour outage is possible and the public needs to be prepared for the impact of that, i.e. spoiled food, unable to go to work, business shutdown, retail outlets for food, fuel, etc closed.
- SCADA systems should allow for ‘user level’ updates to address vulnerabilities found in SCADA devices
- No consensus on an information sharing clearing house being used or available for utility operators. US-CERT and ISAC’s exist at the Federal level.
- Suggested that vendors who service multiple utilities serve as the closest thing to an information sharing environment and could build situational awareness when attacks occur for customers across a number of different business domains
- No formal interface established between utilities and State government agencies
- ISERnet – Infrastructure Security and Restoration Network - DOE information sharing network that utility entities stakeholders can review and update the status of outages
- Policies and procedures should be established for dissemination of information shared between utilities and State agencies to then be disseminated to the public/media
- Would like to see a neutral/3rd party verification for all new utility products or systems
- Define triggers and expectation for ‘cyber Warfare’ outbreaks
 - Department of Defense (DOD) responsibility which includes what the triggers

Inter-State Exercise: Geo Magnetic Storm

Scenario: Geo Magnetic Storm (GMS)

Conducted Wednesday October 19th, 2011, hosted by the National Oceanic and Atmospheric Administration (NOAA)-Space Weather Prediction Center (SWPC) in Boulder, CO.

Participants and Stakeholders in Attendance

AMEC Earth & Environmental, Inc	Hillary King
Black Hills Corporation	Ann Hendrickson Alvin Pinkston
City of Aurora	Porter Ingrum
City and County of Denver	Kevin Magner Patricia Williams
City of Wheat Ridge	Wade Hammond
Colorado Division of Emergency Management	Jason Finehout Kerry Kimble
Federal Emergency Management Agency (FEMA)	
Incident Management Assistance Team	Andrew Batten
Disaster Emergency Communications	Roger Schroder
Colorado Energy Office	Jonathan Miller
Michigan State University	Dr. Roger Koenig
National Oceanic Atmospheric Administration	
University Corporation for Atmospheric Research (UCAR).....	Director - Tom Bogdan
Space Weather Prediction Center (NOAA-SWPC).....	Executive Officer Dianne Suess
Branch Chief	Brent Gordon
Program Coordinator	William Murtagh
Tri-State Generation and Transmission Association, Inc	Dave Sayles
U. S. Department of Energy.....	Katherine Kweder Alice Lippert
Western Electric Coordinating Council	Karl Fittinger
Xcel Energy	Pete Judiscak Steven Owen

Introduction

The Inter-State exercise was a discussion-based, no fault table-top exercise. The GMS exercise was attended by a wide range of local, State, regional and Federal stakeholders including a special appearance from the Department of Energy. It began with a presentation by William Murtagh, Program Coordinator, about Space Weather and the processes established for the SWPC to monitor and analyze potential impacts from a space weather event. A history of past solar storm events that affected areas from the Rocky Mountains to the Caribbean, and an actual GMS in 1989 was then presented to establish the viewpoint that such an event could occur today. Injects were delivered giving stakeholders and participants the opportunity to respond by discussing actions and processes that would be implemented. Before continuing on with the next inject, the participants discussed amongst one another the potential for other secondary impacts. Prior to closing the exercise, a panel discussion was held with subject matter experts to answer questions and discuss the severity of the scenario and the likelihood of Colorado impacts. The EA Exercise Coordinator collected comments, suggestions, concerns and recommendations throughout the exercise and from the hot-wash that followed. To give the reader a better awareness of Geomagnetic Storm conditions, the following sub-section details the uniqueness of solar weather activity and the potential for high hazardous impacts on Earth should a solar flare or coronal mass ejection (CME) be detected in a direct path toward Earth. It is with this understanding that the Exercise Design Team decided a Geomagnetic Storm scenario would be most appropriate for the Inter-State Exercise.

Understanding Solar Weather and Geo Magnetic Storm Impacts

The North American Electricity Reliability Corporation (NERC): *Critical Infrastructure Strategic Roadmap (October 2010)* identified three HILP risks that warrant increased attention: coordinated physical attack, coordinated cyber attack, and severe Geo Magnetic Disturbance (GMD).

Threat: Along with major earthquakes, severe geomagnetic storms (GMS) are among the least predictable high impact/low probability natural hazards that the Nation faces. Some latitudes are more susceptible than others. Colorado is somewhat geographically protected, but could equally be at risk for major impacts. At the low end of the threat spectrum, small geomagnetic disturbances are frequent events and the bulk electric system is experienced in dealing with an incoming occurrence. At the extreme end of the spectrum, however, recent experience does not exist for analysis. The likelihood and potential severity is unknown, and the effectiveness of operational responses and mitigation steps is uncertain. Considerable work is underway to better understand space weather phenomena and the impacts on the electric grid, but substantial uncertainties are likely to continue.

Cause: Geomagnetic storms are caused by periodic solar activity, particularly large solar flares and associated coronal mass ejections (CMEs) that create disturbances in the near-earth space environment. CMEs hurl up to billions of tons of particles at speeds of hundreds of thousand

miles per hour toward earth's outer magnetic field. When a CME is projected in a direct path toward Earth, this "solar wind" plasma impacts the magnetosphere causing rapid changes in the configuration of the earth's magnetic field, a form of space weather called a geomagnetic storm (GMS). These storms create geomagnetic induced currents (GICs) that can seriously disrupt and permanently damage the bulk power system.

Event History: The strongest solar "superstorm" on record (often referred to as the Carrington event) occurred in 1859 well before high voltage power grids were established. Even with the relatively primitive telegraph lines of the times, the incoming GIC on telegraph wires ignited fires and shocked telegraph operators. The aurora was seen as far south as Mexico and Cuba.

A more recent solar storm in 1989 caused the HydroQuebec system to collapse within a few seconds as equipment protection relays tripped in a rapid cascade of events. Six million people were without power for up to nine hours that it took to bring the system back to 83 % of capacity.

Preparedness Challenge: The challenge for risk managers is that there are no reliable methodologies for estimating the likelihood of an especially severe GMS on the scale of the 1859 event.

Probability of Occurrence: The sun goes through a regular cycle of activity of roughly eleven years. It has been unusually quiescent for the past few years, but is anticipated to reach the next cyclical maximum (solar max 24) of sunspot and GMS activity in 2012-2013. CMEs are roughly coincident with sunspot activity, but assumptions vary widely about the periodicity of potentially catastrophic storms. Best guesses are that the probability of occurrence is about every 100-500 years. Earth may be well overdue for such an occurrence or because of its unpredictability, the next catastrophic solar storm may not occur for hundreds of years. At this time there is no statistical basis for estimating its maximum likely strength.

Exercise Elements

Exercise Design Team

The GMS Exercise Design Team was made up of staff from the SWPC, the EA contractor team members, the PUC, DEM and CEO, and members who participated on the Intra-State exercise – cyber attack. The SWPC played a key role in developing injects appropriate to simulate the impacts received from an actual solar weather occurrence.

Setting

Solar weather activity has increased. The SWPC is on a heightened alert status, which requires 24/7 data monitoring. A series of solar flares have been detected over the past few days.

Objectives

The objectives of the GMS exercise were to explore preparation, protections, response and recovery from a GMS on electric utility infrastructure and other critical infrastructure.

- Explore the hazards of Solar Weather to utilities
- Discuss potential vulnerabilities
 - Generation
 - Transmission
 - Transformers
 - Communications
- Explore defenses and safeguards utilities have in place
- Explore implications of Smart Grid technologies
- Explore implications of renewable technologies
- Look for opportunities/methods to share information

Scenario

The scenario began with the detection of increased solar storm activity that had potential to impact Earth. To better educate the participants and stakeholders learning what processes would continue in monitoring the increased activity. Injects then quickly escalated from increased solar storm activity to a direct solar flare impact to Earth causing a Radio Blackout 5 (R-5) level event. Stakeholders discussed the processes that would occur at this level of impact and what would be affected. To better understand the implications of a higher magnitude solar weather impact, the scenario increased Earth's exposure to a Solar Radiation Storm (S-5) level. The stakeholders discussed processes, protection measures, and the levels of impacts, temporary and permanent, that would require response and recovery and restoration operations. The two-day event was compressed into a 5 hour exercise. Infrastructure affected at this level of exposure would include satellites rendered useless where memory impacts cause loss of control including Global Positioning Systems making navigation near impossible, radiation exposure to astronauts, crews and passengers in flight, intermittent or fluctuation in voltage, accidents due to interruption of electric power continuity (traffic lights, mass transportation systems), blackout of high frequency communications, massive back-up generated power needs, complications with pumping of liquid fuels, potential for collapse of the grid if the level of exposure continues to rise. Discussion revealed aspects of Colorado's natural protection from GMS because of its geographical location and other features.

Exercise Results

Strengths

- Major utilities have monitoring and prepping processes in place and would be initiated immediately after SWPC warning notification
- Radio communications are integral to energy sector operations, as R-hazard approaches (typically much earlier than S-Scale impacts), utilities would have to adapt. However, R-Scale disruptions would primarily be an impact to HF radio, not cell phones or over-air television broadcasts
- Utilities believe that the SWPC and WECC lead time on notifications allow them to make the necessary preparations and precautions to avoid damage to infrastructure. There are also automatic fail safes on voltages surges to protect equipment if manual action is not taken.
- Most backup generation and micro grid would not be affected. The voltage is too low, and there is not a significant amount of metal in the ground to produce Geomagnetic Induced Current (GIC)
- Colorado does not have 768 KV high voltage transmissions lines, Colorado lines are in the 400 KV range. The 768 KV transmission lines are more susceptible to GIC
- Cell phone infrastructure and service would not be impacted by the S, R or G storms
- In the scenario presented, a single GMS storm, utilities believe that recovery would be quick, in a matter of hours, as long as infrastructure protections and fail-safe's work and infrastructure are not damaged. Compare this event to a snow storm where tree's fall on power lines, or a tornado where power lines and poles are downed, there is less infrastructure damaged in this type of event
- If utilities turn off their transformers, causing wide spread blackouts, to protect their equipment, an outage of 4-8 hours will have little impact on communications or other emergency backup power systems. Once the outage extends to 12 hours and beyond, such localized power redundancy becomes impacted

Capability Gaps

- HF radio typically used by utilities as a secondary/backup communications system, not the primary system, so R-Scale impacts to energy sector would probably not cause major impacts alone.
- Sectors that rely heavily on High Frequency-band communications are aviation and marine transport. Satellite communication can be disrupted, including GPS satellites. This could knock out service to PDA's and SatPhones/satellite TV/satellite internet. Combined with HF-band disruption, could significantly impact air and marine operations.
- SWPC: ACE Spacecraft (Advanced Composition Explorer) would be impacted by GMS event, would provide detailed input for subsequent alerts/warnings. Spacecraft is over 15 years old, well past its original service life. Spacecraft is fairly robust, but can be knocked out by extreme space weather. If this occurs, it is a big one! It would prevent gathering detailed information for further solar hazards until brought back online. President has proposed funding for a replacement. Deep Space Climate Observatory, which may be up by 2014.
- Geomagnetically Induced Current (highly damaging to energy/pipeline components) does not always reach damaging levels at the onset of a GMS event. May occur or suddenly spike without warning minutes or hours into event
- Some natural gas meter stations have back-up power generation capability, but it's possible to restore pipelines manually, it's just more difficult taking longer to restore delivery. Often gas transmission pipelines are powered by gas, so they are self-supporting
- In 1989, Quebec operators did not have ground current monitoring, could not respond in time. (Unconfirmed)
- Even with ground current monitoring, sudden GMS spike could overwhelm mitigative measures. Areas at mid-latitudes (Colorado) may be particularly vulnerable because they typically do not have ground current monitoring.
- Liquid Fuels Issue: most utilities and many public agencies and private companies use the same suppliers for diesel. It will be an issue if everyone is on back-up power generation
- Some healthcare facilities do not have backup power. Local EMs would attempt to address, and pass problems up the chain. (Most likely aged or non-acute facilities. Hospitals performing surgery or acute care have back-up power generation capabilities in place)
- Replacement of transformers creates number of issues if replacement is required
 - The supply of transformers is 100% overseas
 - Majority of transformers are custom made
 - Demand will drive up prices and extend delivery
 - There may be competition with foreign countries in the transformer market
 - Delivery time is between 18-24 months in a non-event period (unknown if demand spikes)
- SWPC relies on satellite – ACE and the future Deep Space Climate Observatory. A large storm has potential to knock out the satellite and leave earth with little warning of future storms for a number of years until a new satellite could be deployed. Proposal, budget approval, build and launch will take at least 5 years.

Issues

- The Space Weather Prediction Center, WECC and major utilities are cautious about issuing an alert of a G-Scale storm due to the 'Cry Wolf' scenario.
- SWPC believes it has the tools to make a prediction that there will be impacts to power, etc. and doesn't want to alert media, utilities, etc. about non-event storms.
- Consumer Protection? What about food and agriculture impacts?
- Component Damage: There has been discussion about strategic component stockpiles. Most utilities keep spares, but not for all transformers/components. Lead time to order new components typically as high as 18-24 months, only available from overseas vendors
- Purchase of spare components like large capacity transformers could cost as much as \$20 million per unit and lead times for delivery are extensive.
- Edison Electric Institute (EEl) has a voluntary spare transformer program
- Transformers are difficult to transport and requires permits
- Stockpiled transformers also have significant storage costs and maintenance requirements
- Tri-State pre-stages some spare components, but few
- SWPC: Suggests assessment of supply chain vulnerabilities. NERC reports on the subject have been "dire"

Recommendations

- Utilize information sources on solar weather warnings
 - Space Weather Prediction Center (emails)
 - Energy Assurance Daily (Web site)
 - Western Energy Coordination Council (WECC)
 - Recommend to monitor and update this section of the Plan
 - Recommend monitoring programs and advocate cost recovery for utilities which build redundant equipment into their protection plans.

Western Region Energy Assurance Exercise

November 29th through the 30th, 2011, sponsored by the Department of Energy (DOE) and the National Association of State Energy Officials (NASEO)

Introduction

The Western Regional Energy Assurance Exercise was structured to engage participants in active discussion through three energy emergency scenarios. This was done in order to help participants identify gaps or areas where further planning and process improvements are needed in developing energy assurance plans. The exercise also served as an excellent opportunity for Federal, State, local and industry participants to jointly discuss energy emergency planning and response.

Western Region Energy Assurance Exercise, Phoenix, AZ

Colorado Attendees

- City and County of DenverPatricia Williams
- City of Lakewood, EA Contractor SAIC Steve Brodsky
Brian Nielsen
- City of Wheat Ridge Wade Hammond
- City of Aurora and Wheat Ridge
represented by EA Contractor AMEC Earth & Environmental..... Jeff Brislawn
- Colorado Division of Emergency Management (listed by rank) Kerry Kimble
Jason Finehout
- Colorado Energy Office Jonathan Miller
- Tri-State Generation and Transmission Association Allan Wick

*Exercise Elements***Setting**

To stimulate a meeting about the current state of affairs

Pre-exercise Discussion

- 1) American Samoa seismic activity, tsunami and power outages
- 2) Economic petroleum crisis
 - a. High prices outcry
 - b. \$175 a barrel in Nov 2011, leveled out at \$100 a barrel
- 3) Expectations on State Energy Offices
- 4) Prolonged cold weather in northern states
 - a. Spiked heating costs
- 5) Cyber threats and attacks to infrastructure on the rise
- 6) Heightened threat level on cyber attacks on infrastructure
- 7) Trucker strike due to petroleum prices
 - a. Consumer goods, foods, delivery timeframes disrupted

Objectives and Evaluations

Participants were numbered off and grouped so that each participating State and/or Territory was represented in each breakout rooms as thoroughly as possible. Discussions were to take place on each scenario to evaluate how the scenarios would impact their State, Territory, cities and counties, and the overall region.

Highlighted Issues of Concern:

- How would State and local government and industry evaluate the emergency event and its impacts?
- How would preliminary assessments of the magnitude and duration of the emergency be developed?
- What response measures would participants take in the event of such an emergency?
- What interdependencies pose the greatest concern and why?
- In their energy assurance plans, have States and localities considered impacts similar to those from the scenarios?
- What lessons have State and local participants learned as a result of these emergency scenarios, and what actions may they take within their organizations to improve their energy assurance?

Scenarios

1. A 9.0 magnitude “Cascadia” earthquake and resulting tsunami
2. Cyber attacks to the petroleum and natural gas infrastructures with cascading impacts on the electric infrastructure in the Western region
3. Truckers’ strike impacting petroleum supplies

Scenario #1 – Cascadia Tsunami

Colorado Impacts

Although Colorado was not directly impacted by the tsunami itself, cascading secondary impacts were realized.

- The State Emergency Operations Center would be activated to implement the Emergency Management Assistance Compact (EMAC) to help systematically deploy resources to the Pacific Northwest impacted regions.
- Regional Balancing Authorities would coordinate with their Northwest counter-partner to assist in assessment, restoration and recovery operations depending on establishing a priority restoration process.
- The Colorado Energy Office along with the DoRA – Public Utilities Commission would serve as an ESF #12 Co-Lead Agency to CDEM for assistance.
- Other infrastructure systems impacts and needed resources would be handled through the appropriate ESF at the SEOC.
- Colorado would/could experience impacts at all levels affecting the economic structure of the State for an extended timeframe.
 - Petroleum delivery disruption (much liquid fuels resources would/could go to the Northwest for recovery operations)
 - Inflation on products and produce from the Northeast
 - Costs of resource mobilization (should CO deploy resources)
 - Impacted banking and finance networks, circulation of money
 - Cyber networks vulnerability and rerouting necessities

Scenario #2 – Cyber Attack: 42 million people without power

Colorado would be severely affected by the magnitude of this scenario. With the volatility of power restoration, critical life-saving facilities would have to rely on back-up power generation. A good analysis of which entities are backed-up doesn’t really exist from a state level. Individual municipal and county government operations may have a better perspective on what is backed-up in their area. Larger medical-related service facilities are, but smaller ones are not. Critical measures would have to be activated immediately if the entire state was expected to be powerless even for more than a few minutes. Each municipality, county, and State level

operations would be activated to ensure that public safety was protected and resources could be deployed accordingly.

Heaviest impacts (not in priority of severity)

- Liquid Fuels operations, pumping capabilities failure;
- Electric and Natural Gas power delivery failures
- Critical government and life-saving services
 - Adequate fuel for **all** back-up generation
 - Feeding and Sheltering operations to accommodate “all” special needs populations
 - In-Home critical health needs response operations
 - Food and agriculture refrigeration and operations capabilities
 - Public Health and Environment laboratory facilities impact
 - Information Technology services within government facilities
 - Public Information processes for keeping the affected public informed
- Water/Waste Water systems
 - Water pumping stations
 - Waste Water systems processes
- Banking and financial networks failure
 - Financial transactions incapability
 - Money circulation issues
 - Credit card processing
- Transportation systems operations (traffic lights, light rail, bus systems, railway transportation, air travel – Denver International Airport)
 - Transportation of fuels, rescue operations, recovery operations severely hampered
- Public Information and media access failure
- Economic impact (business operations failure)
- Military installations operations

Impact Assessment and Recovery Operations of the Cyber Network

- Cyber security investigation and assessment going on behind the scenes (at each entity and at a regional level) to quickly solve the point of failure(s)
- Recovery may be a patch-work process on many fronts to temporarily get operations back up and running, then a more intensified evaluation of what it will take to fix the cascading problems will ensue.
- Cyber Working Groups will organize and evaluate at the larger impact perspective

Scenario #3 – Independent Trucker Strike

Colorado would certainly be affected if an Independent Trucker Strike were to occur and continue for any length of time. There are several large truck stops throughout Colorado, but

particularly concentrated in the Denver Metro area. Colorado's attendee from the City of Wheat Ridge Police Department stated that Travel Center of America Truck Stop in Wheat Ridge was the largest one in the Denver area. His city would be greatly impacted by a trucker strike.

Local Considerations

- Increased police protection in case of a civil disruption
- Pre-staging in preparation for civil disturbance
- Ask for State and other jurisdiction Law Enforcement back up manpower
- Assessment of fuel availability for government fleet, law enforcement, fire and EMS operations
- Preparedness to provide for lack of delivery of produce, water, baby formula, dairy, and meat items to local grocers
- Public/Private negotiations between city and fueling stations to assess fuel allocation consideration for public use

State Considerations

- State Fleet fuel reserves assessment
- Monitoring for State resources should civil disturbance occur
- Early negotiations between State Colorado Energy Office and fuel supply/markets
- CEO potential to act as a mediator between truckers and fuel supply (if that is possible for temporary reduction in diesel fuel costs to alleviate situation)
- Review transportation fuels policy, practices, programs and establish early relationships with appropriate contacts

Lessons Learned from Western Region Energy Assurance Exercise

- Liquid Fuels is a key component to EAP
 - CEO plans to hire a Transportation Fuels Specialist upon return from exercise and update Liquid Fuels Plan
- State level planning with other States and regions
 - Utilize resources like the Western Governors Association
- State level Cyber Security. Realization that it is a global concern.
 - Cyber Security Working Groups should be established if not already done so
 - Include cyber security personnel in exercises and planning functions
 - Monitor Federal guidelines for cyber security in electric utilities
 - Advocate that utilities have in place securities at least at the level of Federal guidelines
 - Be prepared at the State level (PUC) to establish cyber security guidelines should it be placed within the State’s authority to monitor/regulate
- Continue to clarify roles and responsibilities between the stakeholders during an energy emergency to streamline response and recovery activities
- Continue planning sessions with the Energy Assurance Advisory Group at least on a quarterly basis
- Use ISERnet and other official sites for monitoring Energy Assurance information

Summary

Through the exercises and the overall EA Planning process a better understanding of the organizations and agencies involved has resulted in a refined collaboration between public and private energy stakeholders. The need for continued planning in HILP exercise scenarios is evident and vital in understanding the potential impacts and cascade system failures that occur from catastrophic and many times unexpected incidents. The energy sector is complex in its interdependent systems. It is recommended that CEO, in collaboration with DEM, develop a list of critical services identifying those that have back-up power generation and to what level of capacity. This information could be added to the energy sector assets GIS Database for added value and use during an actual energy emergency event. When considering critical infrastructure, expanded knowledge and cross-training strengthens the system of response and recovery by adding redundancy. Best practices can then be standardized and implementation becomes integrated into daily activities.

Book 3A

Hazard Typology and Quick Reference Guide TM

Book 3A is a comprehensive typology of both natural and human-caused hazards that goes beyond a simple list of threats. Based on critical energy infrastructure assets and their relative risk and vulnerability to specific hazards, a rating scale and risk composite score ranking was developed to demonstrate general probability of impact to the energy sector from each hazard listed. The top seven natural hazards identified as priority threats by the EAAG are listed first as opposed to an alphabetical presentation.

Book 3A Table of Contents

X. Hazard Typology	1
Introduction	1
Definitions and Terms	2
<i>CEAEP Energy Sector Impact Score (ESIS)</i>	<i>4</i>
<i>Risk Composite Score (RCS)</i>	<i>5</i>
<i>Natural Hazards</i>	<i>10</i>
<i>Drought</i>	<i>13</i>
<i>Flood</i>	<i>18</i>
<i>Lightning</i>	<i>23</i>
<i>Tornadoes</i>	<i>26</i>
<i>Windstorms</i>	<i>30</i>
<i>Avalanche</i>	<i>33</i>
<i>Wildfire</i>	<i>36</i>
<i>Extreme Heat</i>	<i>42</i>
<i>Hailstorms</i>	<i>43</i>
<i>Precipitation</i>	<i>46</i>
<i>Thunderstorms</i>	<i>47</i>
<i>Winter Weather</i>	<i>49</i>
<i>Earthquake</i>	<i>51</i>
<i>Erosion and Deposition</i>	<i>54</i>
<i>Expansive Soils</i>	<i>56</i>
<i>Landslides/Mudflows/Rock falls</i>	<i>59</i>
<i>Landslides/Mudflows/Rock falls</i>	<i>59</i>
<i>Subsidence</i>	<i>64</i>
<i>Solar Weather/Geomagnetic Storm</i>	<i>67</i>
<i>Volcanic Activity</i>	<i>69</i>
<i>Human-Caused Hazards</i>	<i>72</i>

<i>Crime versus Terrorism:</i>	74
<i>Criminal Exploitation of Critical Infrastructure:</i>	76
<i>Nuclear Attack</i>	86
<i>Radiological Attack</i>	92
<i>Explosive Attack</i>	94
<i>Chemical Attack</i>	98
<i>Biological Attack</i>	103
<i>Physical Attack</i>	108
<i>Cyber Attack</i>	112
<i>Electromagnetic Pulse (EMP) Attack</i>	118
<i>Major Transportation Accident or Disruption</i>	121
<i>Dam failure</i>	127

The CEAEP is a comprehensive document that includes background information, reference materials, and other subject matter that may not be of interest to all readers. As a convenience, suggested sections are identified below for specific audiences.

For State Agencies and Local Emergency Management Stakeholders

- Hazard Typology
- GIS Natural Hazard Overlay Maps

For Utilities

- Hazard Typology
- GIS Natural Hazard Overlay Maps with Top 7 Hazards

X. Hazard Typology

Introduction

Hazard typologies provide category models and systematic classifications of hazards within these models. Hazard reference guides are subject-matter reference and decision-support tools which define and provide a general or specialized description of the hazards a jurisdiction may face. This Hazard Quick Reference Guide combines some of the functions of a typology and reference guide, and is intended primarily as a general reference and decision-support document to:

- Provide a basic typology and classification of potential hazards to energy infrastructure and delivery in Colorado
- Succinctly describe and provide general information on hazards with potential to disrupt energy infrastructure or delivery in Colorado
- Provide an introduction to hazards and potential impacts on interdependent critical infrastructural systems, focusing on intra and inter-sector interdependencies involving energy sector operations
- Within the scope of the CEAEP project, present information specific to the energy sector and its interdependent sectors within the State of Colorado, or reference information relevant to the management of an energy emergency in Colorado
- Develop an approximate ranking system contextualizing the relative risks posed by the selected hazards to energy operations in general, and potential risks to energy operations in Colorado whenever possible within the scope of the CEAEP research process

Note that the scope of this document does not include specific or customized recommendations regarding preventive or mitigative approaches to the selected hazards, nor does it provide customized consequence analyses. Further developments and updates to the CEAEP and other relevant documents to include customized vulnerability and risk assessments, asset security and engineering assessments, and threat reduction/customized mitigation planning, is recommended.

The typology format employed in the Colorado Energy Assurance Emergency Plan resembles the typology, hazard profiles, and consequence analyses established by The Colorado Division of Emergency Management in the 2011 revision of the *State of Colorado Natural Hazards Mitigation Plan*. However, the full range of hazards relevant to energy assurance is not limited to natural phenomena alone. This typology therefore includes two primary hazard categories: Natural and Human-Caused, with entries further describing the type of hazard and a brief selection of potential consequences for each. Research methodology includes document reviews including after action reports, cost reports and studies, state-maintained emergency management and hazard mitigation documents, stakeholder interviews and consultations, primary source review selected from relevant open-source literature, and consultation with subject matter specialists.

Definitions and Terms

Geographic Extent

Regarding geographic location and extent, potential hazard impacts may range from global, national, US-regional, statewide, state-regional, or localized. Therefore, a hazard with simultaneous potential impacts throughout multiple countries in different regions of the world would be termed "*Global*," and a hazard with simultaneous potential impacts on a wide area of The United States would be termed "*National*." Likewise, a hazard with simultaneous potential impacts on the States of Florida, Mississippi, and Georgia would be termed "*US-Regional*." A hazard with simultaneous potential impacts on areas within the entire State of Colorado would be termed "*Statewide*." Further, a hazard within the State of Colorado with simultaneous impacts on multiple counties representing a significant geographic area and/or population would be termed "*State-Regional*," and a hazard with potential simultaneous impacts limited to a relatively small geographic area or population would be termed "*Localized*."

In the Hazard Quick Reference Guide below, geographic extent per hazard refers to the probable maximum geographic extent for each type of hazard, and the maximum likely impact zone at the highest level of hazard severity, but this does not preclude the same type of hazard impacting smaller geographic areas. For some hazards, geographic extent includes two entries, the first representing the greatest potential geographic extent of the hazard, and the second representing a typical geographic extent of the hazard. For computational purposes, the greater geographic extent entry is utilized.

General Impacts

Estimates of potential hazard impacts are based on review of previous events and/or available sources and research studies which forecast the severity of potential events for which there is not a significant historical record available. A hazard with potentially extreme consequences likely to overwhelm available response and recovery resources within the impacted area is termed "*Catastrophic*." A hazard with the potential to produce heavy costs and highly disruptive consequences within the impacted area is termed "*Severe*." A hazard with the potential to produce substantial costs and significantly disruptive consequences within the impacted area is termed "*Moderate*." A hazard with the potential to produce relatively minor costs and disruptions is termed "*Slight*." General Impacts include potential human injury, illness, and loss of life, as well as economic costs and disruptions to critical infrastructure, services, and commerce. However, for the purposes of this reference guide, *the General Impacts (GI) category primarily refers to impacts that do not specifically pertain to the energy sector*. Potential impacts that relate specifically to the energy sector are estimated in the Energy Sector Impact Score (ESIS) described below.

Neither the GI or ESIS categories are exhaustive, and may not include every potential impact, but are intended to provide basic background information to support decision-making relevant to an Energy Emergency. General Impact (GI) entries listed in the Hazard *Quick Reference Guide* below, *refer to maximum estimated impacts*, and do not preclude the same type of hazard producing lower impacts.

Probability

Estimates of potential hazard probability are based on previous records of the same or similar hazards, and research and analysis of the conditions under which the hazard is likely to develop. Hazard probability is not based on specific or time-sensitive information regarding projected incidents, but is based on analysis of the general conditions conducive to the hazard's development. Conditions conducive to any specific hazard may change significantly over time, these hazard probability estimates should therefore be reviewed and updated periodically. Hazard probability may vary widely depending on a variety of geographic, economic, social, and political factors. Therefore, *probability is estimated based on the likelihood of impacts specific to the State of Colorado*. Furthermore, hazard probability assessment is complicated by the nature of certain hazards which are guaranteed to occur, but only over an extremely long timeline. An example of one hazard of this type is super-volcanism in the Yellowstone Caldera, which will certainly have catastrophic or severe impacts within the State of Colorado when it does occur, and is guaranteed to occur at some future point, but for which the probability of occurrence in any given year is extremely low. As a result of the difficulties inherent in estimating the probability of hazards that are guaranteed, but which occur on a geologic timeline, for the purpose of this analysis, *hazard probability will be limited to a period of twenty five years into the future from the time of this document's development*. A hazard which is virtually guaranteed or extremely likely to impact the State of Colorado in any given year within this twenty five year time-frame is termed "*Certain*." A hazard with significant potential to impact the State of Colorado within this time frame is termed "*Very Likely*." A hazard with some potential to impact the State of Colorado within this time frame is termed "*Moderately Likely*," a hazard with low potential to impact the State of Colorado within this time frame is termed "*Rare*," and a hazard with a very low potential to impact the State of Colorado within this time frame is termed "*Extremely Rare*."

CEAEP Hazard Typology Rating Scale

The CEAEP Hazard Typology Rating Scale combines the terms and definitions above, to produce a snapshot of each hazard along a series of six axes including Geographic Extent (GE), General Impact (GI), Previous Occurrences (PO), Future Probability (FP), Energy Sector Impact Score (ESIS), and Risk Composite Score (RCS). The Hazard Typology Rating Scale is neither comprehensive nor definitive, and a hazard's position on any axis of the scale alone is not intended to determine priorities for prevention, mitigation, response, or recovery activities. Rather, the Hazard Typology Rating Scale is a decision-support tool intended to quickly and

efficiently provide decision-makers with a baseline summary of each hazard and its potential impacts on energy assets and services in the State of Colorado.

Table X-1 CEAEP Hazard Typology Rating Scale

Geographic Extent	Potential Impact	Previous Occurrences	Future Probability	Energy Sector Impact Score (ESIS)	Risk Composite Score (RCS)
<i>Global</i>	<i>Catastrophic</i>	<i>Frequent</i>	<i>Certain</i>	<i>Catastrophic-Systemic</i>	<i>xx/100</i>
<i>National</i>	<i>Severe</i>	<i>Regular</i>	<i>Very Likely</i>	<i>Catastrophic</i>	
<i>US-Regional</i>	<i>Moderate</i>	<i>Periodic</i>	<i>Moderately Likely</i>	<i>Severe</i>	
<i>Statewide</i>	<i>Slight</i>	<i>Rare</i>	<i>Rare</i>	<i>Moderate</i>	
<i>State-Regional</i>		<i>Extremely Rare/None</i>	<i>Extremely Rare</i>	<i>Slight</i>	

Source: Center for International Security Policy and Research (CISPR), 2012

CEAEP Energy Sector Impact Score (ESIS)

The Energy Sector Impact Score (ESIS) is a category of the CEAEP Hazard Typology Rating Scale which estimates a hazard's potential maximum impacts to energy assets and infrastructure, potential maximum disruption to energy services and delivery that might result. Estimates of potential impacts to the energy sector may vary considerably depending on information available, and some ESIS results may be calculated with substantial information regarding specific impacts to energy sector assets in Colorado, and some with only generalized information regarding the types of damage or disruption that similar hazards have produced, or studies and simulations have forecasted. For hazards that are rare, speculative, or for which there is no open source Colorado-specific consequence analysis available, ESIS is therefore a generalized calculation. This effect is compounded with regard to forecasting the impacts of potential hazards for which there is little or no historical precedent, or for deliberate human-caused hazards like terrorism and other criminality, which may involve tactical and strategic targeting processes which perpetrators calculate to be difficult for policymakers and law enforcement to forecast. ESIS is a general ranking system that is primarily estimated from previous cases, case studies, incident records, official documents, technical manuals, scientific journals, sponsored seminars, workshops, surveys, subject-matter specialist consultation, and other open source materials. With the exception of confidential stakeholder feedback, all supporting materials are open source (OSINT). As a result, the ESIS estimates should not be considered reliable indicators of specific threats to the grid, or particular critical infrastructural vulnerabilities, nor should they be considered a primary forecasting or cost-estimation metric. Rather, the ESIS is an estimation of potential impacts to energy infrastructure or disruption of services based on the potential maximum impacts of the hazard combined with open source and other relevant data

reviewed during the CEAEF development process which enables a general estimate of potential hazard severity as it relates to the energy sector and energy delivery in Colorado.

Risk Composite Score (RCS)

The Risk Composite Score (RCS) is a numeric value assigned to each hazard, which combines the entries for each of the previous categories into a composite maximum per-hazard value of 100.00. The entries for Geographic Extent (GE), Future Probability (FP), Previous Occurrences (PO), General Impact (GI), and Energy Sector Impact Score (ESIS) are combined to calculate the per hazard Risk Composite Score. Category entries are not weighted equally, and category weighting systems vary between natural hazards and human-caused hazards. For both hazard sub-types, estimates of potential energy sector-specific impacts (ESIS) are privileged with the greatest weighting. For natural hazards, maximum geographic extent of the hazard (GE) and future probability (FP) are privileged with greater weighting in the final RCS calculation, while general impacts not directly relevant to the energy sector (GI), and previous occurrences (PO), are incorporated into the RCS calculation with lesser weight. For deliberate human-caused hazards, the (ESIS) and (GE) categories remain privileged, with a lesser weight assigned to previous occurrences (PO), and a proportionally greater weight assigned to future probability (FP). Note that the difficulties inherent in attempting to reliably model and forecast deliberate hazards renders the (FP) designation for deliberate human-caused hazards a simple proxy combining two relevant factors: general upward or downward trending in deliberate threats attempted or carried out, and estimates of conditional conduciveness to the threat and the numbers and types of actors most likely to carry it out. Within-category entries are assigned weights in equally distributed proportion to the number of possible entries in that category. For example, for the (ESIS) category entry, the maximum RCS point value is 50.00, and there are six possible entries ranging between *Catastrophic-Systemic* at the highest end of the scale, to *Negligible* at the lowest end of the scale. Therefore, the highest severity ESIS entry of *Catastrophic-Systemic* would contribute 50.00 points to a hazard's Risk Composite Score, while the lowest ESIS entry of *Negligible* would contribute 8.33 points to the hazard's Risk Composite Score.

Figure X-1 Risk Composite Score Calculation

The Risk Composite Score (**RCS**) calculation is expressed below

If (**PO**) = Previous Occurrences
 AND (**GE**) = Maximum Geographic Extent
 AND (**FP**) = Future Probability
 AND (**ESIS**) = Energy Sector Impact Score
 AND (**M**) = Maximum category RCS points
 AND (**E**) = Category Entry
 AND (**N**) = Number of possible category entries
 THEN:

$$\frac{E_{PO}(M)/N + (E_{GE}(M)/N) + (E_{FP}(M)/N) + E_{ESIS}(M)/(N)}{100}$$

= RISK COMPOSITE SCORE

Center for International Security Policy and Research, 2012

The Risk Composite Score is not intended to rank hazards in terms of severity, impact to the energy sector, previous occurrences, general impact, or probability alone, but is a composite value that reflects the general estimates within all of these categories. As a decision-support tool, the Risk Composite Score is best viewed in conjunction with the hazard summary as well as external and scenario-dependent information, to produce a holistic decision-making framework. The Risk Composite Score should therefore not be viewed in isolation, as the significance of the Risk Composite Score to decision-makers may vary depending on emergency management phase and scenario-specific decision-making priorities and objectives.

The weighting of compositional categories in the Risk Composite Score can produce final scores that must be contextualized with specific category information. For example, because potential impacts to energy sector assets and capabilities (ESIS) is the most heavily-weighted category, hazards with potentially extreme energy-sector impacts may receive a high Risk Composite Score despite very low probabilities of occurrence. Likewise, hazards with a high frequency of occurrence and significant general impact, may receive a relatively low Risk Composite Score due to the hazard's relatively low potential to specifically impact energy sector assets and operations.

The weighting of compositional categories in the Risk Composite Score can produce final scores that must be contextualized with specific category information. For example, because potential impacts to energy sector assets and capabilities (ESIS) is the most heavily-weighted category; hazards with potentially extreme energy-sector impacts may receive a high Risk Composite Score despite very low probabilities of occurrence. Likewise, hazards with a high frequency of

occurrence and significant general impact, may receive a relatively low Risk Composite Score due to the hazard's relatively low potential to specifically impact energy sector assets and operations. It is important to note that the RCS ranks hazards in terms of relative risk.

RCS scores rank potential hazard impacts and probabilities relative to other hazards in this reference guide. RCS scores do not provide absolute rankings capable of forecasting the probability of hazards relative to other hazards not included in the reference guide, or of providing reliable probabilities of a hazard occurring at all, or having specific impacts and costs if it does occur.

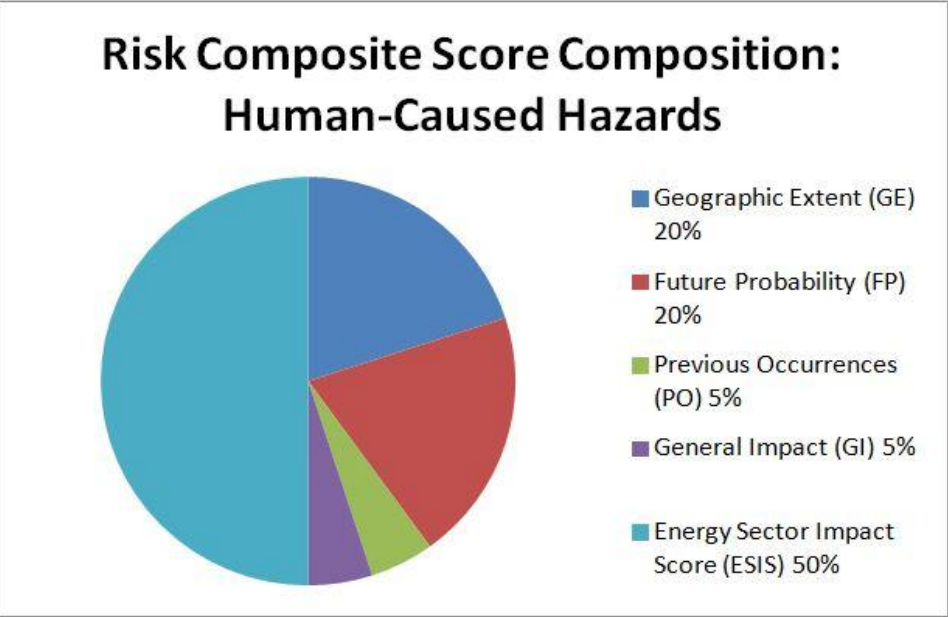
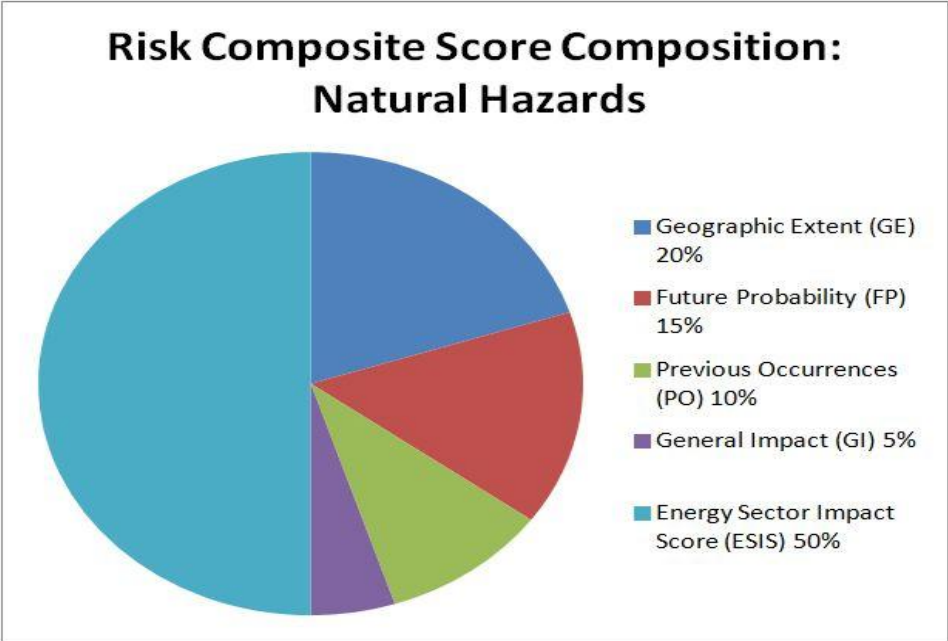


Table X-2 Risk Composite Score Rankings for Natural Hazards and Human-Caused

Natural Hazards		
RANK	EVENT	RISK COMPOSITE SCORE
1	Volcanic Activity*	80.00
2	Winter Weather	75.41
3	Thunderstorm	75.41
4	Tornado	67.99
5	Wildfire	65.41
6	Solar Weather/GMS Event*	64.76
7	Flood	64.74
8	Precipitation	63.83
9	Earthquake*	63.26
10	Lightning	62.50
11	Extreme Heat	61.83
12	Windstorm	57.16
13	Landslide/Mudflow/Rock fall	49.16
14	Erosion/Deposition	47.57
15	Avalanche	45.49
16	Expansive Soils	43.82
17	Subsidence	43.39
18	Drought	43.41
19	Hailstorm	40.49
<i>(*) Indicates high impact/low probability event</i>		

Human-Caused Hazards		
RANK	EVENT	RISK COMPOSITE SCORE
1	Cyber Attack	84.41
2	Electromagnetic Pulse Attack*	73.33
3	Major Transport Disruption	67.08
4	Physical Attack	60.83
5	Nuclear Attack*	58.26
6	Explosive Attack	55.41
7	Biological Attack	55.00
8	Dam Failure/Sabotage	53.74
9	Chemical Attack	34.99
<i>(*) Indicates high impact/low probability event</i>		

Hazard Quick Reference Guide™

Natural Hazards



Natural hazards refer to naturally-occurring phenomena with the potential to negatively impact human populations. When natural hazards substantially impact human populations or activities, they may produce a *natural disaster*. The term natural disaster therefore refers to specific incidences in which natural hazards produced significant and costly impacts on humans and human activities. Further, when any hazard or series of hazards produces impacts that temporarily or permanently overwhelm all available response and recovery capacities in affected jurisdictions, they may be deemed *catastrophic*.

Therefore, under this typology, hurricanes are a natural hazard, but 2007's Hurricane Humberto was a natural disaster, and 2005's Hurricane Katrina was a catastrophic natural disaster. This definition of catastrophic disasters as phenomena which overwhelm response and recovery capabilities should not be confused with insurance industry standards, which classify a catastrophe as any natural disaster which causes more than \$25 million in damage to insured property, regardless of impact on response and recovery capacities.

Natural hazards may be interrelated, or may combine to produce or exacerbate additional hazards. For example, seismic phenomena like earthquakes may have ruinous impacts when they occur in isolation, but a sufficiently powerful earthquake occurring in a vital location may produce substantial secondary hazards like tsunamis, subsidence impacts, avalanches, mudslides, or rock falls. Likewise, prolonged drought impacting regions of the United States may produce significant secondary economic impacts, and prolonged droughts in vulnerable areas of the developing world can potentially produce serious secondary impacts such as famine and civil disorder.

Consistent with the hazard typology developed in the State of Colorado Natural Hazard Mitigation Plan, natural hazard sub-categories identified as particularly relevant to the State of Colorado include:

- | <i>Atmospheric</i> | <i>Geologic</i> | <i>Other/Unclassified</i> |
|---------------------------|-----------------------------------|----------------------------------|
| ✓ Drought | ✓ Avalanche | ✓ Wildfire |
| ✓ Extreme Heat | ✓ Earthquake | |
| ✓ Floods | ✓ Erosion & Deposition | |
| ✓ Hailstorms | ✓ Expansive Soils | |
| ✓ Lightning | ✓ Landslide/Mudflow/Rockslide | |
| ✓ Precipitation | ✓ Subsidence | |
| ✓ Thunderstorms | ✓ Solar Weather/Geomagnetic Storm | |
| ✓ Tornadoes | ✓ Volcanic Activity | |
| ✓ Windstorms | | |
| ✓ Winter Weather | | |

The first seven hazards of the Hazard Quick Reference Guide™ were considered to be the biggest threat from natural hazards to the energy sector assets and infrastructure. They are listed out of normal alphabetical sequence and are not categorized by type (atmospheric, geologic, or other) because of their importance relative to the energy sector. These selected natural hazards are accompanied by a companion book of Natural Hazard Overlay Maps which depict selected energy assets located in the hazard zones. The maps are made available for official use only and are not viewable within this document. Contact the Colorado Energy Office or the Division of Emergency Management for official access. The Natural Hazard Overlay Maps were developed by Patrick Engineering, Inc. in support of the CEAEP project. The methodology used to produce these maps and tables is included with the maps.

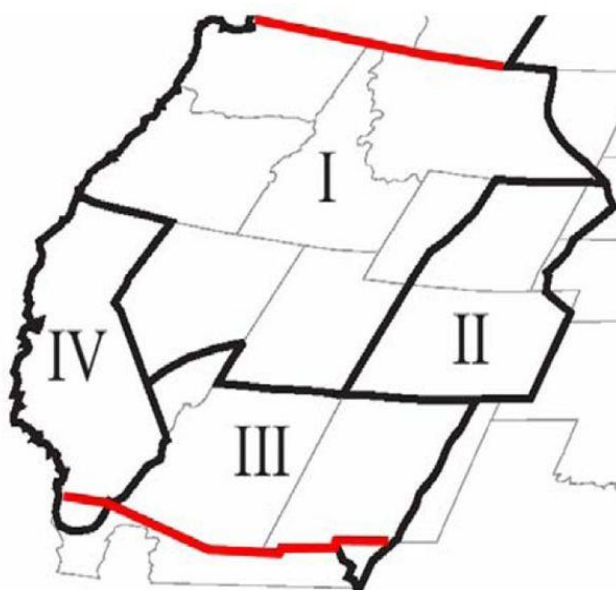
Drought

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
US- Regional/Statewide	Severe	Periodic	Very Likely	Negligible	43.41

General Summary: Extended periods of low water supply are referred to as Drought. Drought is a regularly recurring hazard in virtually all locations in the State of Colorado, and across wide regions of the western, mid-western, and southern United States. Drought may present quickly at any time of year, or may develop gradually over a period of months. Drought may occur over entire US regions to include Colorado, or may be localized to a relatively small region within the State of Colorado. Droughts may be short term or long term in duration.

Potential Impacts: Drought may produce an average of 3-4 deaths per year, and is not projected to substantially impact most critical services or facilities. However, drought may strain water resources and produce significant economic impacts within the agricultural sector, and if severe enough to require municipal or industrial water use restrictions, may produce economic impacts within additional market sectors including but not limited to: mining, liquid fuels extraction, heavy manufacturing, and retail services. Drought occurring in some areas may increase the risks and potential impacts of wildfires in wildland-urban interfaces.

Western Electricity Coordinating Council System Areas:



Source: Poch, Conzelmann, and Veselka. "An Analysis of the Effects of Drought Conditions on Electric Power Generation in the Western United States." National Energy Technology Laboratory, April 2009

Energy Sector Impact Score: *Negligible*. Depending on the impacted area's electric power mix and a range of circumstantial factors, the impacts of drought can vary considerably. The energy sector relies substantially on water resources, with more than 39% of all water withdrawals in the U.S. being for electrical generation. However, the majority of energy sector water use is full cycle, and therefore returns the water to the environment, making the energy sector vulnerable to drought, but not a significant contributor to secondary drought impacts. Transmission and distribution infrastructure are generally not impacted, but thermal power plants and plants utilizing water or steam turbines can lose generating capacity. Severe droughts most typically

occur during peak electrical demand season, sometimes exacerbating impacts to the energy sector. According to simulations, in a severe drought year, hydroelectric generation across the WECC system can theoretically drop by up to 30%. If drought is severe enough to result in water shortages or serious water management issues, hydroelectric, coal, and nuclear generating facilities can also be impacted, as they rely on significant surface and ground water resources for turbine generation or cooling. Within the WECC system, more than 94% of generating facilities that draw surface or ground water for cooling are coal fired, and less than 6% of the water drawn for generation facility cooling is for natural gas facilities. In Colorado, as within the WECC system, the prominence of natural gas in the western United States electric power mix can effectively mitigate against drought, provided good coordination between operators exists. It is expected that natural gas generating output could therefore be increased to cover the load during severe drought conditions in Colorado or throughout the WECC system, however, this may have secondary consequences such as shortage or price increase in the natural gas and electricity markets, as natural gas generation is ramped up substantially to compensate for loss of capacity in hydroelectric, coal, or nuclear generation facilities. Because hydroelectric, coal, and nuclear generation rely heavily on water supply, regions and states with electric power mixtures heavily reliant on hydroelectric, coal, and/or nuclear generation may be moderately to severely impacted, particularly if they do not have excess natural gas generation capacities available to compensate.

Table X-3 Significant Droughts in Colorado

Dates	Impact Areas & Severity
1890-1894	East of the mountains; severe
1898-1904	Southwestern Colorado, very severe
1930-1940	Widespread, prolonged, and severe drought--- The “Dust Bowl”
1950-1956	Front Range; severe
1974-1978	Statewide; driest winter ever recorded in the High Country (1976-77)
1980-1981	Mountains and western slope; inspired the “Colorado Drought Response Plan”
2000-2003	Statewide, multi-year; very severe

Drought in Colorado

1930-1940 Dust Bowl: An unusually moist weather pattern dominated the Great Plains in the decades leading up to 1930. Hundreds of thousands of settlers flocked to the region to take advantage of fertile farmlands. Beginning in 1930, a prolonged drought caused top soils to erode, with the resulting dust storms and desertification leading to the displacement of

Baca Co., Colorado, Easter Sunday 1935

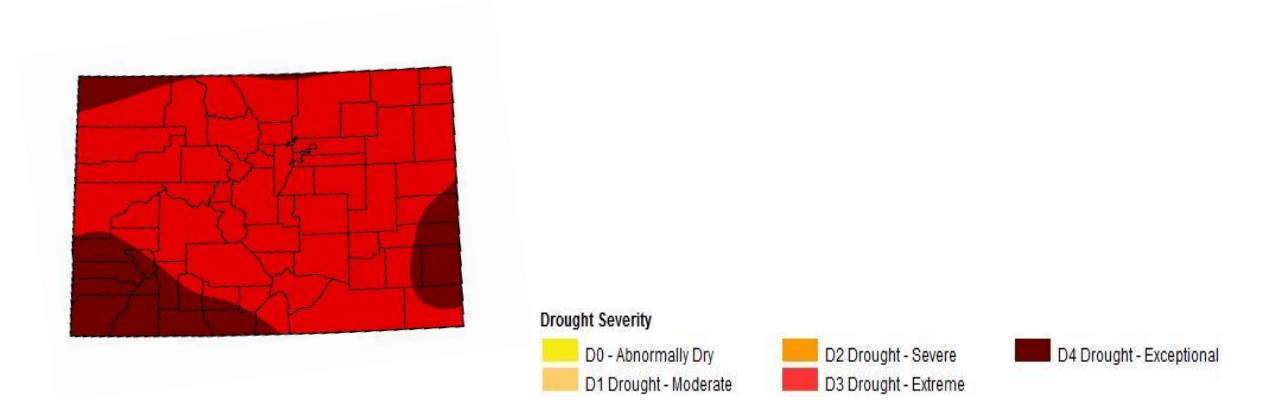


over 500,000 American citizens. In Colorado, the Dust Bowl drought was the longest lasting drought in the state’s history; developing in 1931 and peaking by 1935.

Modern agricultural techniques preserve top soils and anchored vegetation. A 21st century Dust Bowl is highly unlikely. However, an extended drought is possible with the potential for depleting water reservoirs and increasing the risk of wildfire.

2002 Drought: The figure below is the National Drought Monitor Drought Severity Map for August 27, 2002. Drought conditions in every county were classified as either “D3- Extreme” or “D4-Exceptional”. In April 2002 the Colorado Drought Mitigation and Response Plan activated all eight Drought Impact Task Forces for the first time in the history of the program.

Figure X-2 National Drought Monitor Severity Map



The Colorado Energy Office and local utilities identified high-risk power transmission lines while mitigation efforts were undertaken to reduce the risk of wildfire in these areas. At the time, all of the state’s transmission lines were rated “minus 1” meaning that power continuity was assured if any single transmission line was impacted. Snow pack run-off levels were also monitored closely to measure the impact of the 2002 drought on downstream hydroelectric production.

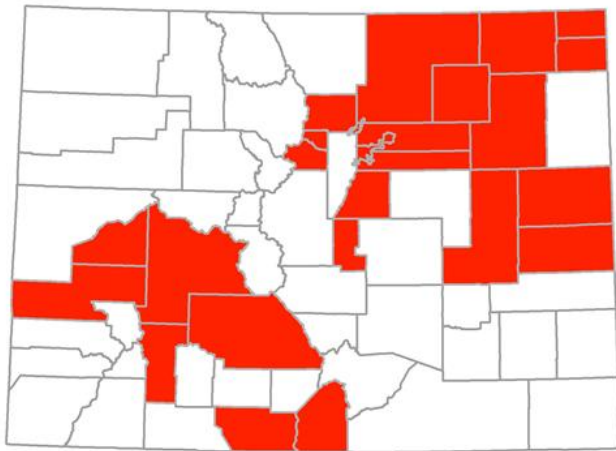
Colorado’s agriculture industry suffered large losses as a result of the 2000-2003 drought. Damages were estimated at \$150 million for ranchers and \$300 million for farmers. A Secretarial Emergency Disaster Declaration from the USDA was awarded to all 64 counties for the first time in over twenty years. In addition, the state of Colorado faced one of the worst wildfire seasons in the state’s history in 2002 with 3,409 wildfires and \$70 million in insurance losses.

Energy Asset Inventory and Drought¹ Using the 2010 Colorado Hazard Risk Analysis, twenty-five high drought risk counties in Colorado were ranked by comparing their energy asset inventory to their drought risk ranking.

Table X-4 County Ranking Of Energy Asset Inventory In Identified High Risk Drought Counties

County	Drought Risk	Transmission Score	Pipeline Score	Substation Score	Plant Score	Hazard Score
Weld	High	4	4	4	4	16
Adams	High	2	2	3	3	10
Logan	High	2	1	2	2	7
Montrose	High	2	1	2	2	7
Boulder	High	1	1	2	3	7
Morgan	High	2	1	2	2	7
Denver	High	1	1	2	2	6
Arapahoe	High	2	1	2	1	6
Douglas	High	2	1	2	1	6
Lincoln	High	2	1	1	2	6
Washington	High	2	1	1	1	5
Kit Carson	High	2	1	1	1	5
Phillips	High	1	1	1	1	4
Sedgwick	High	1	1	1	1	4
Delta	High	1	1	1	1	4
Gunnison	High	1	1	1	1	4
Clear Creek	High	1	1	1	1	4
Cheyenne	High	1	1	1	1	4
Conejos	High	1	1	1	0	3
Saguache	High	1	1	1	0	3
Broomfield	High	1	1	1	0	3
Teller	High	1	1	1	0	3
Gilpin	High	1	1	1	0	3
Costilla	High	1	0	1	1	3
Hinsdale	High	1	0	1	0	2

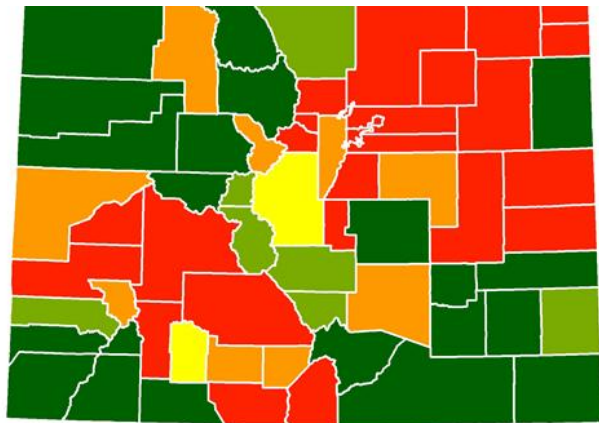
¹ Data, analysis, and GIS maps provided by Patrick Engineering



Identified High Risk County High Drought Hazard Risk Map

High Drought Hazard Counties

Counties in red are classified as High Drought Hazard Risk



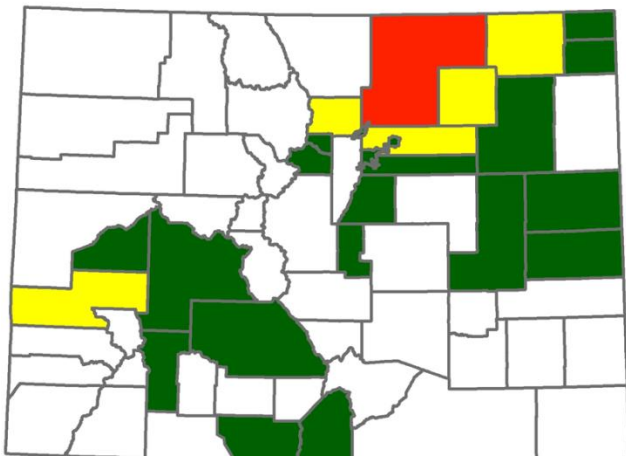
Ranking Drought Hazard Ranking by County

■ N/A
■ Included in plan
■ Low
■ Medium
■ High

Drought Risk by County

Counties in red have the highest Drought Hazard Ranking according to the 2010 Colorado Hazard Risk Analysis.

Counties in orange and yellow have Medium and Low Risk respectively.



Total Score Energy Asset Inventory Ranking in Counties w/ High Drought Risk

■ 2-6
■ 7-11
■ 12-16

High Drought Risk Counties Ranked by Hazard Score

Weld County (in red) has the highest energy asset inventory in a county classified as having a “High Drought Risk”

Flood

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
State-Regional/Localized	Severe	Periodic	Certain	Severe	64.74

General Summary: Flooding refers to the temporary submergence underwater of normally dry land. Flooding occurs when water is introduced to dry land areas in sufficient volume to exceed the carrying capacity of channels, the surface absorbency of the land, or overtop existing hydrologic engineering structures like levees, dams, drainage systems, and aqueducts. Floods are typically attributable to build up of water from snowmelt, precipitation, displacement of water by rock fall or ice jams, or the failure of hydrologic engineering structures. 20-30 significant floods occur on average in the State of Colorado each year.

Potential Impacts: Depending on the causes and geographic area affected, flooding may be slow or rapid in onset, short or long in duration. Colorado's geography renders many areas susceptible to rapid timescale (6 hours>) or "flash" flooding, which may produce dangerous debris-laden swift water capable of sweeping away persons, vehicles, and structures in its path. Floodwaters can produce environmental and public health impacts as chemical runoff drains to waterways and reservoirs, and standing water produces conditions conducive to pathogen and parasite development and spread.

Potential Energy Sector Impacts: *Severe.* Significant volumes of energy assets and infrastructure may be located in floodplains and other flood-prone areas. Floodwaters may damage or destroy any submerged infrastructural asset, and can limit accessibility for emergency response and recovery operations.

Flood in Colorado

1976 Big Thompson River Flood: The Big Thompson River flood of July 31, 1976 was the deadliest flash flood in Colorado history. At least 145 people perished after a stalled thunderstorm produced more rainfall in 24 hours than the region would have normally experienced in an entire year. Water was forced through the narrow canyon at an incredible rate; destroying homes, hotels, campsites and the main artery, U.S. 34, from Estes Park to the canyon's mouth near Loveland.



Debris from the flash flood wiped out all but one of the turbines from the hydroelectric plant at Viestenz-Smith Mountain Park. Federal Disaster Assistance Administration funds were used to rebuild the plant further back from the bank of the river. There was also significant damage to

the Big Thompson dam and a 36 inch steel tube that transported drinking water to the Loveland Filtration Plant. To safeguard against future flash-floods, the river was widened, the highway was constructed higher, and bridges were anchored to strong retaining walls in the canyon. Road construction and unsettled river banks caused rock slides, erosion, and subsidence for years after the immediate disaster.

July 14-18, 1965 South Platte River/Arkansas River Flood: The 1965 South Platte River/Arkansas River event is the costliest flood in the state's history. Unprecedented rainfall caused progressive flooding of the South Platte and Arkansas River basins over a number of days. Unofficial reports from southeast Colorado put rainfall amounts at 15.5 inches in 14 hours at the peak of the storm.

By June 20 the damage extended from north of Ft. Collins to south of Pueblo. Roads were flooded, bridges were washed out, and some of the worst damage occurred in metro Denver on June 16th when flood waters from the South Platte spread to over a half-mile wide or more. At the time, this flood zone represented over 67% of the industrial area in the city and peak discharge was 183% of the previous maximum in recorded history.

In the Denver metro area, both Public Service Company power plants along the river were shut down and emergency circuits became waterlogged and shorted out.



[Rocky Mountain News: June 18, 1965](#)

A pile of debris (trucks, timber, trailers) clogs a bridge at W. Alameda Ave. over the North Platte River. Kalamath St is at the top of the image. The flooded Valley Highway is at the bottom of the image

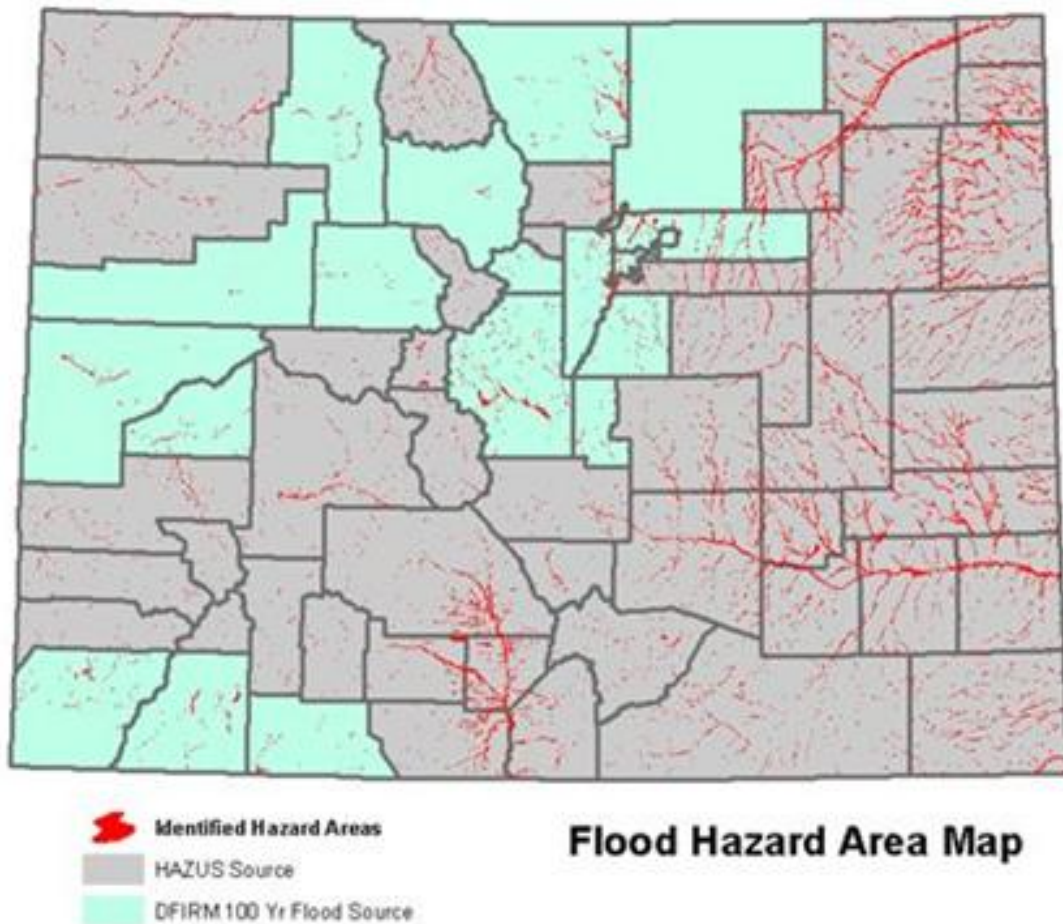
Table X-5 Significant Floods in Colorado Recorded History

Year	Location	Deaths	Damages (in 2007 dollars)
1864	Cherry Creek, Denver	0	\$7,000,000
1896	Bear Creek, Morrison	27	\$8,000,000
1911	San Juan River, Pagosa Springs	2	\$7,000,000
1912	Cherry Creek, Denver	2	\$156,000,000
1921	Arkansas River, Pueblo	78	\$988,000,000
1935	Monument Creek, Colorado Springs	18	\$68,000,000
1935	Kiowa Creek, Kiowa	9	\$20,000,000
1942	South Platte River Basin	n/a	\$10,800,000
1955	Purgatorie River, Trinidad	2	\$47,000,000
1957	Western Colorado	0	\$23,000,000
1965	South Platte River, Denver	8	\$2,600,000,000
1965	Arkansas River Basin	16	\$267,000,000
1969	South Platte River Basin	0	\$28,000,000
1970	Southwest Colorado	0	\$17,000,000
1973	South Platte River, Denver	10	\$505,000,000
1976	Big Thompson Rive, Larimer	145	\$110,000,000
1982	Fall River, Estes Park	3	\$64,000,000
1983	North Central Counties	10	\$34,000,000
1984	West and Northwest Counties	2	\$61,000,000
1993	Western Slope	0	\$2,700,000
1995	Western Slope and South Platte	21	\$68,000,000
1997	Fort Collins and 13 Eastern Counties	6	\$220,000,000
1999	Colorado Springs and 13 East Counties	0	\$130,000,000
2000-6	Statewide various events	5	\$116,801,024
2006	Beaver, Brush Hollow and Eight Mile Creeks	0	\$2,000,000
2006	Horse Creek & West Creek, Douglas	0	\$13,000,000
2006	Vallecito Creek, La Plata	0	\$1,000,000
2007	Chalk Creek Canyon, Chaffee	0	\$1,000,000
2007	Chalk Creek Canyon, mudflows	0	\$2,000,000
2009	Six Mile Creek	0	\$321,000
2010	Statewide flooding, various events	n/a	n/a

Data Source: Colorado Flood Hazard Mitigation Plan 2010

Energy Asset Inventory and Flood² Ten counties in Colorado³ have a Flood Hazard Score of 4 and possess energy infrastructure within a Special Flood Hazard Area (SFHA). A SFHA is defined as an area that will be inundated by a flood event having a 1 percent chance of being equaled or exceeded in any given year. HAZUS methodology is used for counties that were not included in the DFIRM (Digital Flood Insurance Rate Map) database. HAZUS is a national standardized methodology that contains models for estimating potential losses from earthquakes, floods, and hurricanes. It graphically illustrates the limits of identified high-risk locations due to earthquake, hurricane, and floods. Users can visualize the spatial relationships between populations and other more permanently fixed geographic assets or resources for the specific hazard being modeled, a crucial function in the pre-disaster planning process. The following figure shows both HAZUS and DFIRM layered with identified hazard areas.

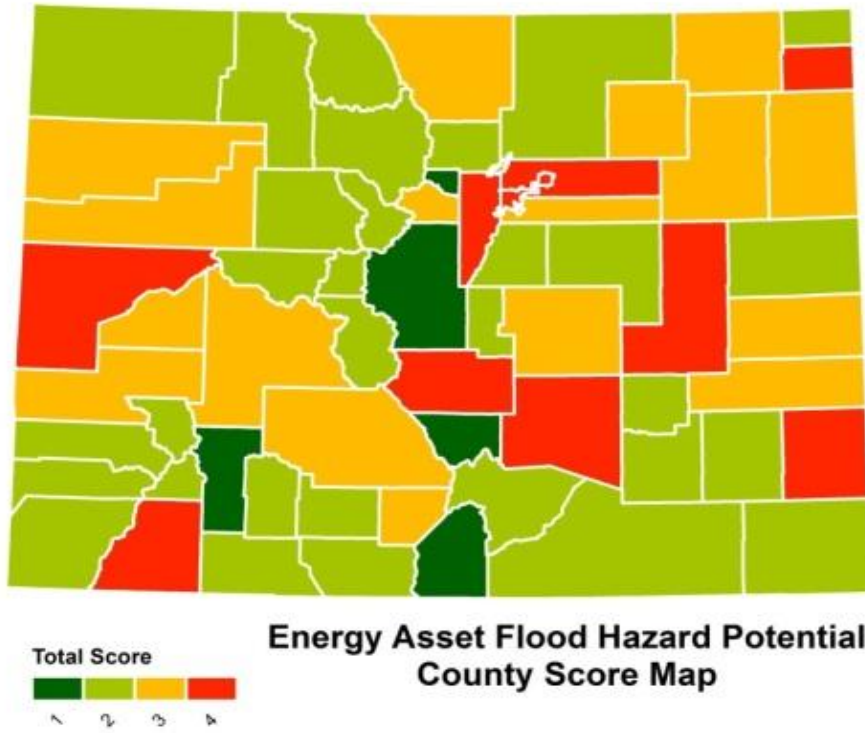
Figure X-3 HAZUS and DFIRM Flood Zones in Colorado



² Data, analysis, and GIS maps provided by Patrick Engineering

³ Adams, Denver, Fremont, Jefferson, La Plata, Lincoln, Mesa, Phillips, Prowers, and Pueblo

Ten counties in the following map have the largest energy asset inventory ranking in high flood hazard areas.



Lightning

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
Statewide	Moderate	Frequent	Certain	Moderate	62.50

General Summary: Lightning refers to electrical discharges produced by electro-static separation of particles within thunderstorm clouds. Lightning is associated with thunderstorm activity, and occurs frequently throughout Colorado. It is most prevalent in the Front Range and high elevation portions of the state, but may occur anywhere in concurrence with thunderstorm activity. In Colorado, peak lightning activity occurs between May-September. Colorado averages approximately 530,000 cloud-to-ground lightning strikes annually, typically resulting in 1-2 fatalities, and 6-7 injuries per year.

Potential Impacts: Lightning poses a serious risk to humans, and often results in injury or fatality when it strikes humans or livestock. From 1995-2009, Colorado ranked 4th in the nation for lightning-related fatalities, with 44 killed during this period. Lightning frequently strikes structures, but rarely causes significant damage and does not directly impact structural integrity. Lightning has killed and injured livestock, and can cause crop damage. Lightning is a common ignition source for wildfires, and thunderstorms involving high winds and lightning activity but low precipitation pose the greatest potential risk of wildfire ignition, particularly when they occur over dry or drought-impacted areas.

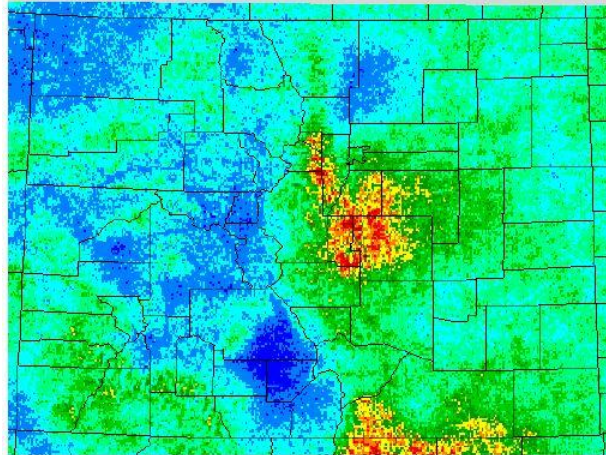


Potential Energy Sector Impacts: *Moderate.* Lightning often strikes electrical transmission and distribution systems. Most lightning strikes impacting the electrical grid result in only minor to moderate property damage, and only occasional minor disruptions to grid operations and electrical services. However, in rare cases lightning strikes can result in significant outages or interruptions. Lightning may pose a significant danger to line workers conducting maintenance operations.

Table X-6 Average Monthly Lightning Flashes for the State of Colorado

Jan	Feb	March	April	May	June	July	Aug	Sept	Nov	Dec
806	1,913	19,404	107,757	596,772	1,258,117	2,001,217	209,775	699,250	5,384	269

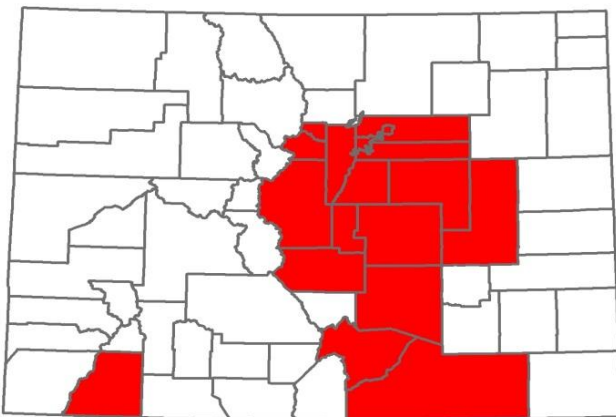
Lightning in Colorado: The greatest flash densities in the state of Colorado occur where the mountains and plains intersect. The Palmer Divide/Pikes Peak Region and the southern Sangre de Cristo mountains are the predominant hot-spots for lightning activity. There are no clear answers as to why this is the case, but leading theories suggest that regions of convergence associated with the mountains/plains circulation might account for this convection. Colorado ranks 26th in the country for lightning flash density.



This figure shows the mean annual lightning flash density for the state of Colorado from 1989-2005 (excluding 2000).

Over 7 million flashes were recorded to produce this image. The annual average total of lightning flashes in Colorado is 6,911,280.

Energy Asset Inventory and Lightning⁴: The following maps compare lightning flash density and energy asset inventory for each county in Colorado. El Paso County has the highest rate of lightning flashes per square mile with an Energy Asset Inventory Score of 13. Alternatively, Gilpin County has the second highest rate of lightning flashes per square mile but a low Energy Asset Inventory ranking. Therefore, it is considered a high lightning hazard area with a lower energy asset impact.

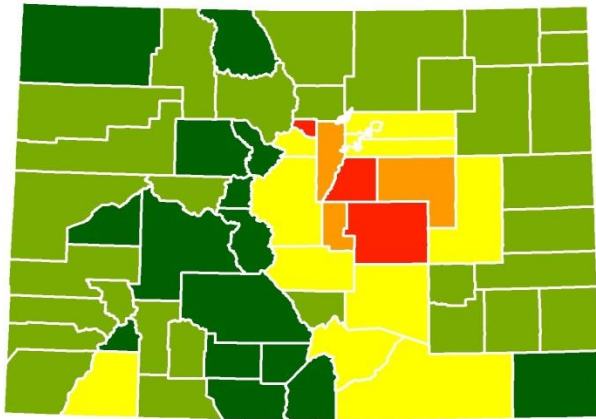


Identified Hazard Areas

Lightning Hazard Map

Counties in red are identified as lightning hazard areas.

⁴ Data, analysis, and GIS maps provided by Patrick Engineering

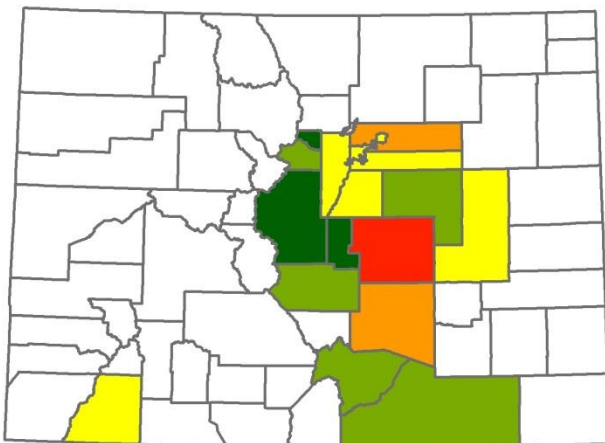


Lightning Strike Density by County
 Average Annual Strikes per sq. mile

1.0 - 3.4	3.5 - 6.0	6.1 - 8.2	8.3 - 10.5	10.6 - 12.9
-----------	-----------	-----------	------------	-------------

Counties in red have the highest lightning strike density (**flashes per square mile**)

- 1) **El Paso County**
27,500 annual flashes
12.9 flashes/square mile
- 2) **Douglas County**
10,900 annual flashes
12.9 flashes/square mile
- 3) **Gilpin County**
1600 annual flashes



County Energy Asset Inventory Ranking in Counties w/ Annual Avg. of >6 Flashes per Sq. Mile
 Total Score

3	4-5	6-7	8-11	12-13
---	-----	-----	------	-------

Counties with an annual average of over 6 flashes per square mile layered with Energy Asset Inventory Scores.

- 1) **El Paso County (in red)**
12.9 flashes/square mile
13 power plants
68 substations
696.2 miles of electric transmission line
213.4 miles of pipeline

Tornadoes

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
State-Regional/Localized	Catastrophic	Regular	Certain	Severe	67.99

General Summary: Tornado refers to localized high velocity rotational winds. Tornadoes are characterized by funnel-shaped debris-bearing clouds extending from storm cells to the ground. Probable damage increases with proximity to the funnel, but hazardous tornadic winds are not limited to the visible debris-laden funnel area. Tornadoes are almost exclusively associated with severe thunderstorms. Tornado severity is classified along the TORRO and Enhanced Fujita (EF) scales. The enhanced Fujita scale rates severity from EF1 (least severe), to EF5 (most severe). All tornadoes are potentially hazardous to life and property, but destructive potential rises precipitously at the EF-3 level and above, with EF3 and higher tornadoes accounting for approximately 6% of recorded tornadoes in the United States, but 75% of tornado-related fatalities. In Colorado, tornadoes may occur anywhere thunderstorms occur, and areas of highest potential tornado activity coincide with areas of highest thunderstorm activity. These areas include the central and northern Front Range foothills extending out through the eastern and northeastern plains. Tornadoes have rarely occurred in other portions of the state.

Potential Impacts: Tornadoes at the lower end (EF-0 through EF-2) of the Enhanced Fujita Scale can push vehicles from roadways, cause superficial damage to vegetation and well-built structures, and cause significant damage to temporary structures and mobile homes. Starting at the EF2 level, severe damage including roof loss may occur in well-built structures, vehicles and other large objects may be lifted from the ground, small objects become missiles, and large trees are downed. At the EF3+ level, most well-built structures may lose all internal walls, rendering above-ground sheltering insufficient to ensure life safety. At the EF 4 level, well-built residences are totally destroyed, and other robust structures are severely damaged or destroyed. Heavy vehicles like airplanes, trains, and semi-trucks can be pushed over or moved short distances. At the EF5 level, destruction of virtually all structures and vehicles will be total, sweeping above-ground residential constructions clear of their foundations, and in some cases stripping asphalt from roadways. Robust above-ground structures may be severely damaged or destroyed, and unreinforced basements become insufficient to ensure life safety.

Potential Energy Sector Impacts: *Severe.* While all tornadoes are capable of damaging or destroying energy infrastructure, the likelihood and severity of potential damage increases substantially at and above the EF3 classification. In Colorado, tornadoes of this intensity are rare but do occur. Electrical generation facilities and substations, transmission and distribution lines,

liquid fuels pipelines, maintenance vehicles and equipment, and other above-ground assets may be impacted.

Tornadoes in Colorado: From 1991-2010 the state of Colorado experienced an average of 53 tornadoes per year; with only 0.4% of those categorized as violent (EF3 and above). The following table shows the number and strength of tornadoes in Colorado from 2000-2010. The majority of these events were categorized as EF0 or ‘Gale Tornadoes’ with the potential to damage chimneys, break tree branches, push over shallow-rooted trees, and damage sign boards.

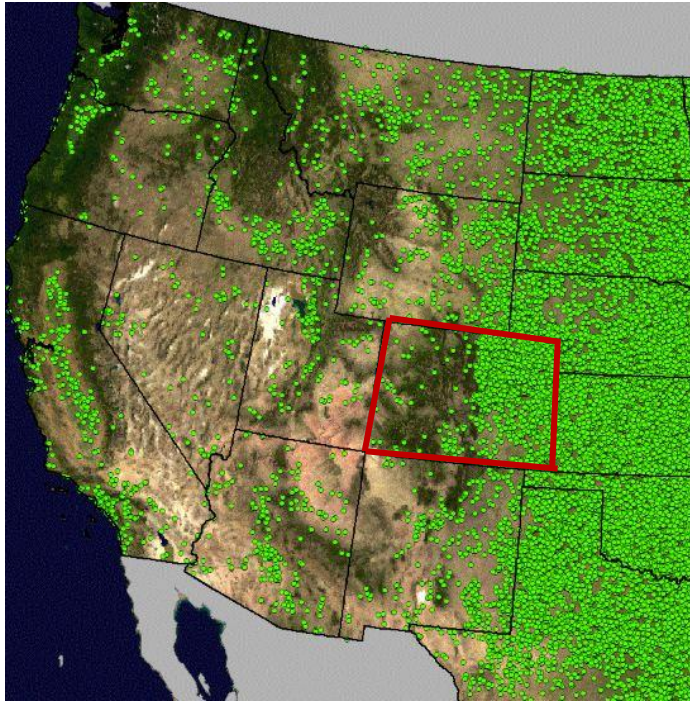
Table X-7 EF0-EF5 Scale Tornadoes in the State of Colorado 2000-2010

Scale	Number	Percent of Total	Wind Speed 3 Second Gust	Tornado Type
EF5	0	0.0%	>200	Incredible
EF4	0	0.0%	166-200	Devastating
EF3	4	0.9%	136-165 mph	Severe
EF2	7	1.5%	111-135 mph	Significant
EF1	48	10.4%	86-110 mph	Moderate
EF0	401	87.2%	65-85 mph	Gale

Source: Colorado Natural Hazards Mitigation Plan 2011

Colorado’s eastern plains are located within the boundaries of ‘tornado alley’ and these counties produce the most tornadoes in the state. The northeastern counties of Weld, Adams, and Washington have experienced well over 500 tornadoes since 1950. In the image below, every green dot signifies a tornado touchdown from 1950-2010.

Figure X-4 US Tornado Touchdowns



Source: NOAA's Storm Prediction Center SVRGIS

The eastern plains of Colorado experience an average of 7 tornado watches per year while the western and central regions of the state average less than one tornado watch per year. From 1950-2010, the state of Colorado recorded 1,778 tornadoes with 5 deaths, 261 injuries, and \$292,778,671 in total damages (property and crops). Prior to 1950, tornadoes in Colorado killed over 40 people.

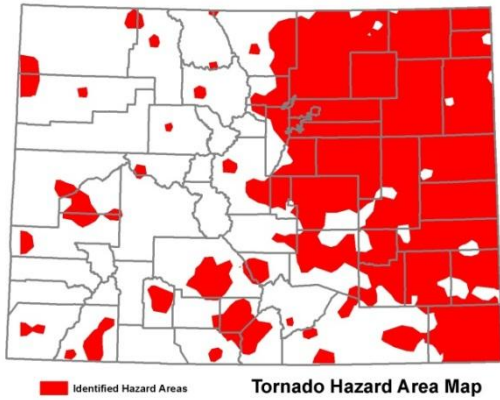
May 22, 2008: Windsor Tornado

Around noon on May 22, 2008 a near mile-wide tornado travelled 35 miles from Gilcrest to west Greeley and north through Windsor, Colorado. This event was categorized as an EF3 tornado with wind speeds as high as 165 mph. The twister injured hundreds of citizens and led to one fatality. At least 80 homes were destroyed and 1,600 structures were damaged. Insurance claims topped off at \$193.5 million, making it the costliest tornado in Colorado’s history.

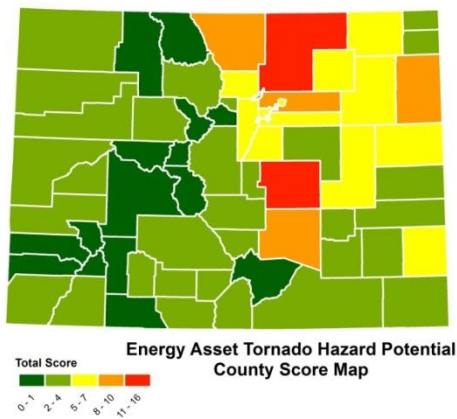


The Windsor tornado damaged at least three power transmission lines; including a pair of 230,000 volt lines at the Fort St. Vrain power plant near Plattville. Additionally, 200 power poles and a half-dozen transmission poles were damaged or destroyed. At least 60,000 citizens lost power as the storm passed through the region.

Energy Asset Inventory and Tornado⁵



The regions shaded in red are identified as Tornado Hazard Areas. These are locations in Colorado where, in the past 60 years, a tornado has been recorded with an enhanced Fujita rating of F0-F5



This map was produced by comparing the Tornado Hazard Area Map on the left with the Energy Asset Inventory ranking of each county in Colorado. Weld and El Paso Counties (in red) have Energy Asset Inventory Rankings of 16 and 13 respectively. These counties also reside in Identified Tornado Hazard Areas.

⁵ Data, analysis, and GIS maps provided by Patrick Engineering, Inc.

Windstorms

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
State-Regional/Localized	Moderate	Regular	Certain	Moderate	57.16

General Summary: Windstorms refer to weather phenomena involving high winds or violent and unpredictable gusts. In Colorado, windstorm events are most frequent in the Front Range and Front Range Foothills, east-central to northeast, and Grand Valley, but may occur anywhere in the state. In summer, warm Chinook winds may descend from the Rocky Mountains and down the Front Range foothills to the eastern plains. Likewise, the interaction of high pressure systems to the west and low pressure systems to the east can cause a Bora, or cascade of heavy winds into eastern and southeastern foothills and plains. Both Boras and Chinook winds may descend from the high mountains through the Front Range canyons and on to the Front Range foothills and eastern plains at speeds approaching or exceeding 100 miles per hour, with sustained 50-80 mile per hour wind speeds being typical.

Potential Impacts: Windstorms can damage roofs and shatter unreinforced windows, down trees, turn unsecured objects into missiles, and blow vehicles from roadways. High profile vehicles are at particular risk, especially when travelling perpendicular to wind direction. Less robust or poorly-maintained structures may be severely damaged or collapse.

Potential Energy Sector Impacts: *Moderate.* Wind storms have frequently downed electrical transmission and distribution lines in Colorado, and will continue to do so. Impacts are generally moderate but occasionally severe, and involve sustained damaging winds across a wider geographic area and for longer duration than most localized thunderstorm or tornado events. Wind storms may complicate maintenance and emergency response operations.

Windstorms in Colorado: According to the Federal Emergency Management Agency, portions of Colorado fall into Wind Zone I (130 mph), Wind Zone II (160 mph), and Wind Zone III (200 mph). The entire Front Range corridor from Cheyenne, WY to Trinidad, CO is classified as a ‘Special Wind Region’.

This region can be seen in the image on the next page where each blue dot represents a recorded wind speed of over 65 knots (approximately 75 mph) from 1955-2011.

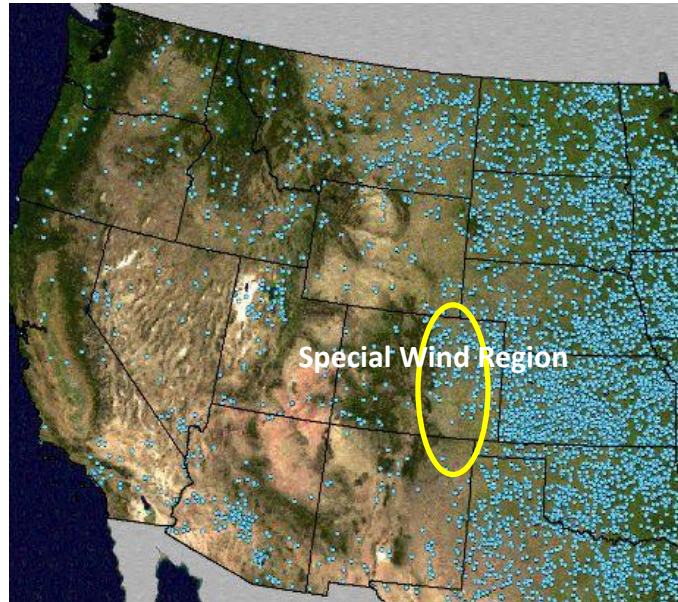


High winds are responsible for toppling this structure next to the Agate Post Office in Elbert County in 2010

From February 21-22, 2012 the Front Range corridor experienced wind gusts up to 90 mph. These winds downed power lines, leaving nearly 45,000 in central Colorado without power. Two wildfires also occurred in conjunction with the wind event.

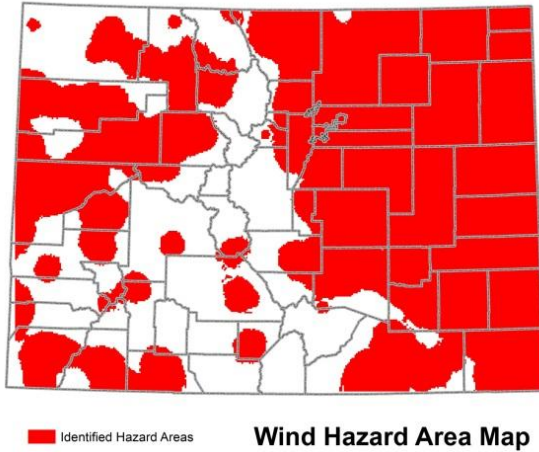
According to the National Climatic Data Center, 3-5 of these types of wind events are typical for any given year. In May 2010, winds gusting up to 75 mph caused power lines to come down in Manitou Springs sparking a grass fire near the Pikes Peak Cog Railway.

Later that month, high winds downed power lines near Conifer and sparked a small wildfire, while power outages were reported in the Big Thompson Canyon and Loveland. Over the past 60 years, windstorms have caused approximately \$367 million in property damage with 21 deaths and 406 injuries reported from 1950 to 2010.

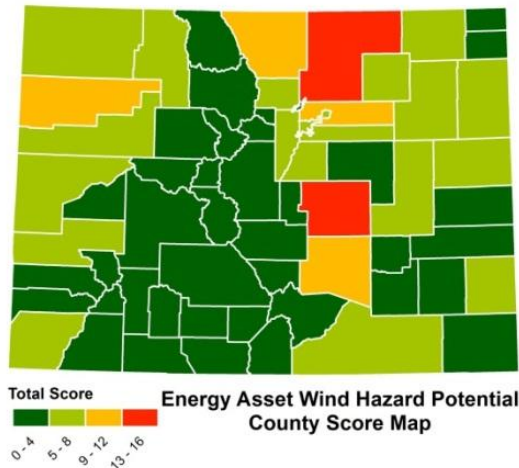


Source: NOAA's Storm Prediction Center SVRGIS

Energy Asset Inventory and High Winds⁶: High wind events may occur in nearly every county in Colorado. Weld and El Paso counties have an Energy Asset Inventory Score of 16 and 13 respectively and both reside within identified High Wind Hazard Areas. From 1950-2010, Weld county experienced 246 high wind events, second only to Larimer county with 293. Additionally, Weld County is home to over 849 miles of electric transmission lines: the most in the entire state of Colorado.



The regions shaded in red are Wind Hazard Areas. These are locations in Colorado where, within the past 55 years, wind speeds have been recorded at 58 mph and above.



This map combines data from the Wind Hazard Area Map (on the left) with the Energy Asset Inventory rating for each county. Weld and El Paso Counties are in red.

⁶ Data, analysis, and GIS maps provided by Patrick Engineering

Avalanche

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
Localized	Moderate	Regular	Certain	Slight	45.49

General Summary: Avalanche refers to snow, ice, and debris flowing rapidly down slope. Avalanches are almost exclusively caused by external stresses on existing snowpack. Onset is rapid. Possible triggers include but are not limited to: precipitation, seismic activity, radiative and convective heating, sudden impacts caused by rockfall, icefall, wildlife, or backcountry recreationists, road or rail activity, timber and mining activity, and explosive blasting. Avalanche paths can be modeled, and high risk areas identified. Avalanches are geographically limited in scope, but pose substantial destructive potential due to the mass, volume, and speed of sliding snow and debris, as well as the air pressure wave which may build in front of the slide and impact persons and structures as it discharges into the run-out and debris deposit zones.

Potential Impacts: Colorado leads the United States in avalanche deaths. Avalanches occur frequently in the high mountain ranges of Colorado, typically occurring in remote and unpopulated areas, and causing no damage or fatalities. Nevertheless, avalanches pose a severe danger to persons, vehicles, or structures in their path, and cause damage and fatalities on an annual basis. Survival rates drop precipitously when victims cannot be extracted within 15-35 minutes. Avalanches may damage or destroy portions of highways and railroads, and bury, crush, or sweep vehicles from roadways and railways. Moderate avalanches may produce snow pressures sufficient to damage or level forests, and cause moderate to severe damage to most structures in their path. Air pressures produced by a moderate avalanche are sufficient to damage walls and blow out doors and windows. Severe avalanches may produce snow and air pressures sufficient to severely damage or completely destroy any structures in its path, and move large objects like boulders and heavy equipment substantial distances. Damage assessment, snow clearing, and debris cleanup can be difficult and costly in avalanche zones. Mitigation measures like erection of barriers and controlled blasting are likewise expensive.

Table X-8 Avalanche Impact Pressure and Damage

<i>Impact Pressure (lbs/ft²)</i>	<i>Potential Damage</i>
40-80	Breaks windows
60-100	Push in doors, damage walls and roofs
200	Severely damage wood frame structures
400-600	Destroy wood frame structures, break trees
1000-2000	Destroy mature forests
>6000	Move large boulders

Potential Energy Sector Impacts: *Slight.* While avalanches can produce severe impacts in affected areas, these areas are limited primarily to high mountain slopes and valleys along avalanche runs. Likewise, while residential and commercial development is discouraged in avalanche zones, some critical energy and telecommunications assets must be located in avalanche zones. By necessity, some service roads to critical energy and telecommunications components may also be located in avalanche zones, and impacts to service roads may hinder access for maintenance and emergency response. Any infrastructural component located in an avalanche zone may be subject to damage or destruction in the absence of mitigative avalanche barriers or other specialized construction.

Avalanche in Colorado:

Peru Creek 2011: In late April 2011, a series of avalanches destroyed 100 year-old trees and a 40 year-old high voltage transmission tower (show in the image on the right) near Peru Creek and the town of Montezuma in Summit County. The Colorado Avalanche Information Center had already warned of an increased danger of avalanche as sensors were recording snowpack levels at more than 160-200 percent of average. Quick warming led to unpredictable avalanches in areas which had not experienced these types of events for hundreds of years.



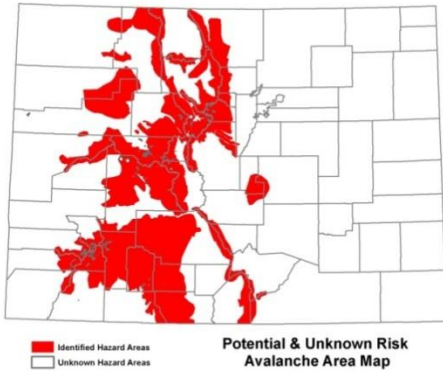
Winter 2012 The winter season of 2012 was equally as dangerous as 2011. High snowpack in the mountains combined with a rapid warming trend during the last half of the winter lead to 6 avalanche-caused deaths during the first three months of the year.

Table X-9 2012 Colorado Avalanche Statistics (Jan-March)

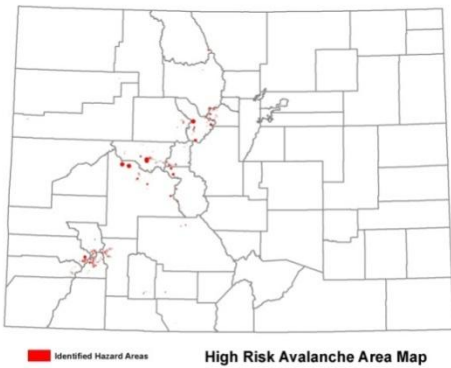
Activity	Caught	Buried	Killed
Skiing	13	7	4
Snowboarding	2	1	1
Snowmobiling	1	1	0
Snowshoe/Climbing/Hiking	2	1	1
Total	18	10	6

Data from the Colorado Avalanche Information Center

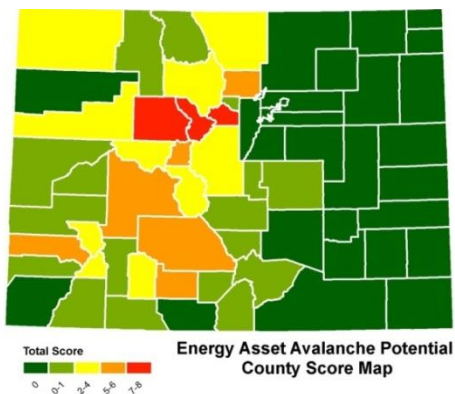
Energy Asset Inventory and Avalanche⁷: The following maps analyze data from historic avalanche occurrences, avalanche paths, and the 10 recreation prediction area zones that are used by the Colorado Avalanche Information Center (CAIC) to forecast avalanches. This information is then compared to the Energy Asset Inventory Ranking of each county in a high risk or potential avalanche area. Areas with a known high risk for avalanche are weighted more heavily than those with potential risk.⁸



Regions highlighted in red are identified as potential/unknown risk avalanche areas.



Regions highlighted in red are high risk avalanches areas.



This map shows the Energy Asset Inventory Ranking of each county in a high risk or avalanche potential area.

Eagle, Summit, and Clear Creek Counties are at the top of the list for potential and high risk of avalanche to energy assets.

⁷ Data, analysis, and GIS maps provided by Patrick Engineering

⁸ These areas are not ALL of the high risk avalanche areas in Colorado

Wildfire

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
Localized	Severe	Frequent	Certain	Severe	65.41

General Summary: Wildfire refers to uncontrolled and undesired combustion of natural and/or human-made fuels. Wildfire may occur in montane, subalpine, foothill, and grassland regions of Colorado, potentially impacting significant portions of all counties in the State. Wildfires may be human-caused in cases of deliberate or accidental fuel ignition, or naturally-occurring. Rapidity of onset and spread is dependent on type of ignition, topography, wind speeds, temperature, humidity, precipitation, and fuel availability. Drier conditions, high winds, low humidity, and high fuel availability are typical contributing factors. In Colorado, wildfires regularly occur during the March-August fire season, but conditions conducive to wildfire development may occur at any time of year. Lightning is the most prevalent natural ignition source. Human-caused ignition may present as a secondary impact of natural hazards in cases of electrical transmission line downing, pipeline damage, or natural gas line damage. Human-caused ignition may also be accidental, in the case of controlled burns that escape containment, or deliberate, in the case of arson.

Potential Impacts: Wildfire onset and spread are highly dependent on a variety of external factors, but damage to structures, vehicles, infrastructure, and improvements is typically severe to catastrophic in impacted areas. Economic losses are highest in wildland-urban interfaces, and may include loss of productivity due to evacuation as well as fire damage. Fatalities are infrequent but do occur.

Potential Energy Sector Impacts: *Severe.* Wildfire may damage or destroy transmission and distribution lines, substations, and other vulnerable facilities and infrastructure. Wildfire may occasionally present as a secondary impact of energy infrastructure damage due to other hazards. For example, windstorms, lightning, and other natural hazards can down transmission and distribution lines, leading to wildfire ignition. Lax vegetation management can result in contact with transmission lines, resulting in wildfire ignition as well as infrastructure damage. High intensity arc flashes can also melt conductors, destroy insulation, and start fires. Wildfire may impact accessibility to energy assets for emergency response and recovery operations.

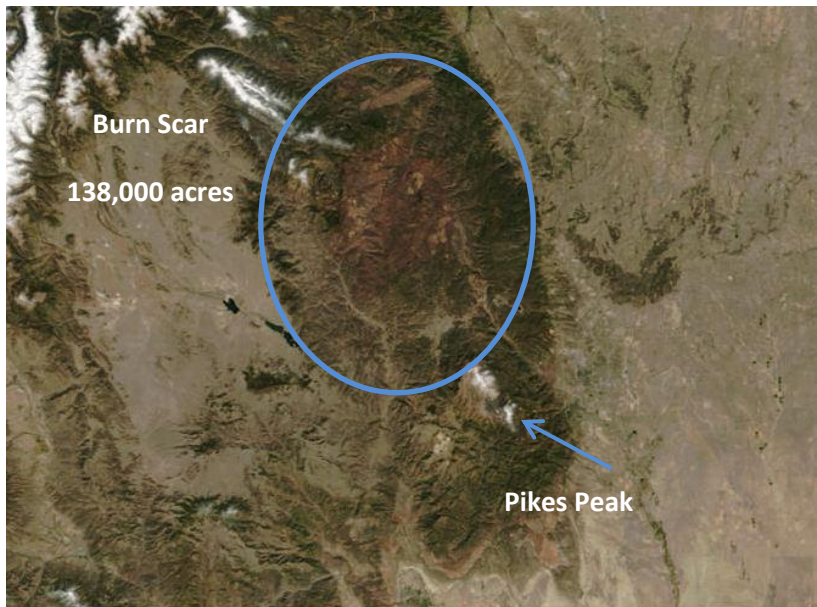
Wildfire in Colorado:

Lower North Fork Fire, March 2012: On March 26, 2012, a controlled burn crossed over a containment line in the Pleasant Park neighborhood near Conifer, Colorado. Sustained winds of 20 miles per hour, gusts of 60 -80 mph, and historically dry conditions caused the fire to grow rapidly and consume 4,500 acres. Eventually, the Lower North Fork Fire destroyed 27 homes. It

is estimated that this fire caused \$1.2 million in utility losses and damaged or destroyed 2-3 miles of electric transmission line.

Fourmile Canyon Fire, 2010:

As the costliest wildfire in Colorado history, the Fourmile Canyon fire destroyed 169 homes and 5 structures. According to the Fourmile Canyon Fire Preliminary Findings revised in October 2011, a total of 474 homes resided within 100 feet of the wildfire perimeter. 168 or 35.4% of these homes were destroyed. Of these, 29 were ignited by crown fire (17.3%) and 139 by surface fire (82.7%). A total of 93% of these homes were destroyed



The Hayman Fire burn scar seen from space in September 2002

within the first 12 hours of the fire. The research team also found that the Fourmile Canyon Fire home destruction scenario followed the same pattern of other wildland-urban interface fires that have occurred in the U.S. The Fourmile Canyon fire also damaged or destroyed at least 225 of Xcel Energy’s utility poles and 15,765 feet of overhead conductor. After containment, many evacuees were still unable to return to their homes due to wide-spread power outages. Xcel energy used a helicopter to deliver poles and restore transmission line to neighborhoods without power. Firefighters were on-hand as lines were energized; at least one small hot spot flared-up during the restoration process.

Hayman Fire, June-July 2002: The Hayman Fire holds the record as the largest wildfire (by acreage) in Colorado’s history. By the end of the event, 138,000 acres had burned and 133 homes were destroyed. This particular event occurred during a historic, state-wide, multi-year drought. Several additional factors contributed to the severity of this event. Thick surface fuels downwind from the start of the fire consisted of deep layers of dry pine needles, shrubs, and bushy, low trees. On the first day of the fire, winds were blowing at 10-15 mph with occasional gusts of 40+mph. By the second day, wind gusts of 50 mph combined with a relative humidity of around 5% resulting in the destruction of 60,000 acres in one day.

Table X-10 Notable Colorado Wildfires 2005-2010 (>1,000 acres burned or homes/structures destroyed)

2005	Mason	11,357 acres
2006	Mauricio Canyon	3,825 acres
2006	Yuma County	23,000 acres
2006	Thomas	3,347 acres
2006	Mato Vega	13,820 acres
2007	Newcastle	1,420 acres
2007	Bear	1,526 acres, 1 home, 2 structures
2008	Ordway	8,900 acres, 14 homes, 10 structures, 3 fatalities
2008	Bridger	45,800 acres
2008	Nash Ranch	1,115 acres, 2 structures
2009	Olde Stage	1,300 acres, 2 homes, 2 structures
2009	Spring Creek	1,340 acres
2010	Parkdale	628 acres, 1 home, 1 structure
2010	Fourmile Canyon	6,280 acres, 169 homes, 5+ structures
2010	Reservoir Road	710 acres, 2 homes, 3 structures

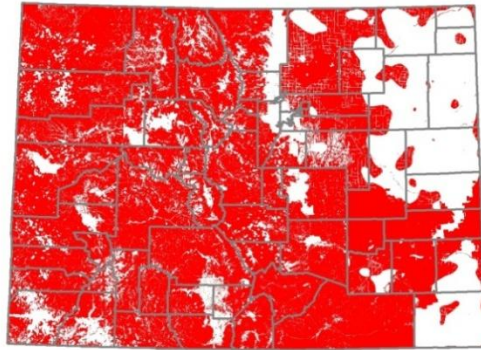
Energy Asset Inventory and Wildfire⁹

The following table lists the 31 counties in Colorado with a total Wildfire Hazard Score of 10 or more. Each county was ranked using an Energy Asset Inventory and Wildland Fire Susceptibility Index layer created from a merged product of two datasets: the Colorado State Forest WFSI Index from 2007 and the Colorado State Forest ‘Colorado Wildland Urban Interface Hazard Assessment’ data from 2002. The first analysis determined the quantity of utilities within the areas valued as “low” or “moderate” risk. The next analysis determined the quantity of utilities within the areas valued as “high” or “very high” risk. High and Very High Risks were weighted more heavily (the energy asset score was doubled). Finally, the Low/Moderate and High/Very High scores were added together to determine the final Wildfire Hazard Score for each county.

⁹ Data, analysis, and GIS maps provided by Patrick Engineering

Table X-11 Total County Ranking of Wildfire Hazard Potential

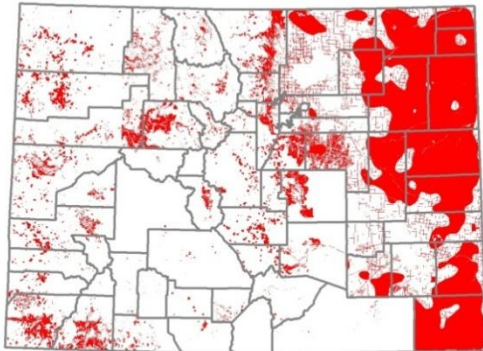
County	Low/Moderate Score	High/Very High Score	Wildfire Hazard Score
Weld	11	16	27
Yuma	2	24	26
El Paso	6	14	20
Morgan	3	16	19
Kit Carson	2	16	18
Mesa	5	10	15
Rio Blanco	7	8	15
Prowers	5	10	15
Logan	4	10	14
Pueblo	8	6	14
Washington	4	10	14
Lincoln	4	10	14
Larimer	3	10	13
Adams	5	8	13
Bent	5	8	13
Phillips	4	8	12
Montrose	6	6	12
Jefferson	4	8	12
Arapahoe	4	8	12
Boulder	4	8	12
Otero	4	8	12
Garfield	5	6	11
Montezuma	3	8	11
Cheyenne	3	8	11
Grand	4	6	10
Routt	4	6	10
La Plata	4	6	10
Archuleta	4	6	10
Denver	4	6	10
Baca	4	6	10
Kiowa	4	6	10



Low to Moderate Wildfire Hazard Potential Area Map
 ■ Identified Hazard Areas

Low/Moderate Hazard Scores were combined with High/Very High Hazard Scores to create this image.

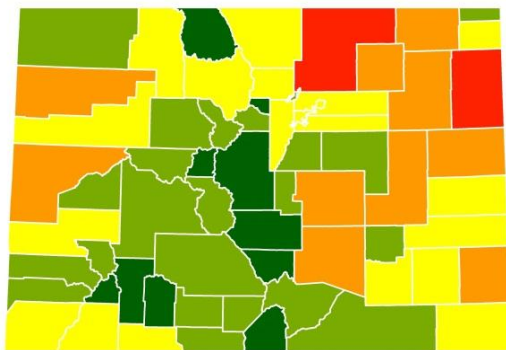
- ✓ Weld and Yuma Counties are highlighted in red with Total Wildfire Hazard scores of 27 and 26 respectively.



High to Very High Wildfire Hazard Potential Area Map
 ■ Identified Hazard Areas

High/Very High Wildfire Hazard Potential Areas are highlighted in red

- Yuma County has the highest energy asset inventory score for a county with high/very high wildfire risk.



Energy Asset Wildfire Hazard Potential County Score Map
 Total Score
 2-5 6-9 10-13 14-20 21-27

Low/Moderate Wildfire Hazard Potential Areas are highlighted in Red.

[View Hazard Overlay Maps Here](#)

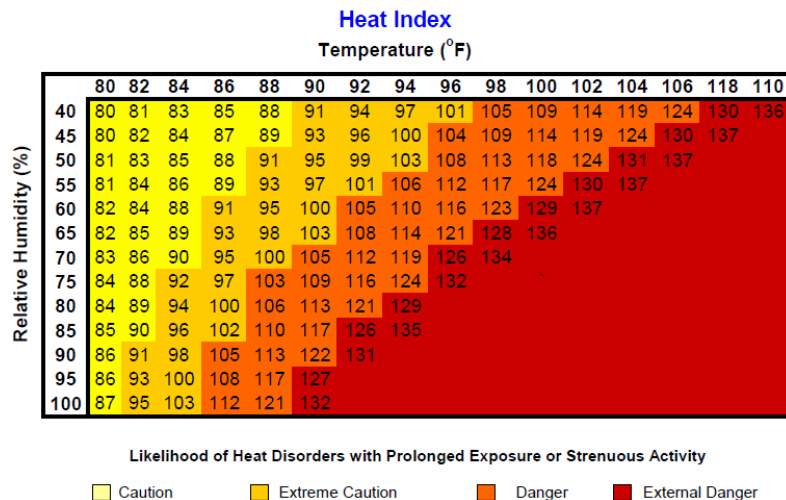
Extreme Heat

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
US-Regional/State-Regional	Moderate	Periodic	Certain	Moderate	61.83

General Summary: Temperatures substantially in excess of the normal high temperatures for the geographic location and season are termed extreme heat conditions. Extreme heat may combine with unusually high humidity, or, may involve extreme low humidity. In the United States, extreme heat accounts for more annual deaths than tornadoes, lightning, and floods combined.

Potential Impacts: Extreme heat often results in relatively high mortality rates within urban areas, with urban elderly being most at risk. Though aviation operators are generally aware of Colorado as a "high and hot" operating area, extreme heat may further decrease air densities, rendering some aircraft operations difficult to conduct safely. Ground transport may be impacted as asphalt roads soften, concrete roads rupture, and railroad tracks are deformed. Extreme heat can stress road and rail transport vehicles, resulting in more frequent mechanical failures. Livestock can be threatened by extreme heat, and agricultural production is slowed and reduced. In the case of extreme heat accompanied by extreme low humidity, wildfires may be more frequent and difficult to combat. Extreme heat increases overall water demand, potentially resulting in water quality and environmental problems, and may compound the challenges of fire suppression.

NOAA's National Weather Service



Potential Energy Sector Impacts: *Moderate.* Electrical grid components may be damaged or overtaxed as increased electrical demand causes power lines to heat and sag. Transmission and distribution lines may fail and/or ignite nearby vegetation, causing service disruptions and potential wildfires. Particularly in urban areas, extreme heat leads to increased electrical demand. In cases of prolonged extreme heat this increased demand could exceed local or regional supply and distribution capabilities, necessitating rolling brownouts or blackouts.

Hailstorms

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
State-Regional/Localized	Moderate	Regular	Certain	Negligible	40.49

General Summary: Hailstorms refer to weather systems that produce precipitation in the form of ice. Hail with a diameter less than 1 inch (quarter sized) is considered non-severe, and occurs frequently in Colorado. Hail is typically rapid onset. The National Weather Service considers hail with a diameter in excess of 1 inch to be severe, with the potential to cause significant damage or injury. In the State of Colorado, severe hailstorms occur most frequently from April-August during the afternoon or evening, and in eastern sections of Colorado which are part of a multi-state area known as "Hail Alley," damaging hail can occur as early as March and as late as October. Front Range, eastern, and northeastern portions of Colorado are most susceptible to hailstorms, with less than 10% of damaging hail falling west of the continental divide. In Colorado, hailstorms result in \$25 million+ in damage approximately three times per year.

Table X-12 Hail Severity by Classification, Size, and Description

Non-Severe Hail	Severe Hail
1/4" Pea	1" Quarter
1/2" M&M	1 1/4" Half Dollar
3/4" Penny	1 1/2" Walnut/Ping Pong Ball
7/8" Nickel	1 3/4" Golf Ball
	2" Hen Egg/Lime
	2 1/2" Tennis Ball
	2 3/4" Baseball
	3" Teacup/Large Apple
	4" Grapefruit
	4 1/2" Softball
	4 3/4"-5" Computer Cd-Dvd

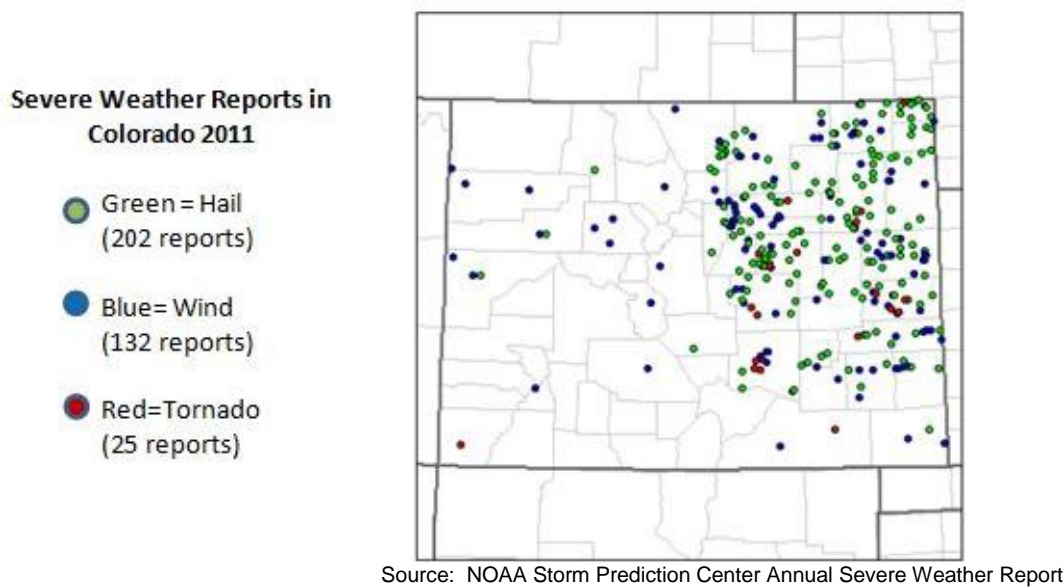
Source: National Weather Service & Colorado Natural Hazards Mitigation Plan 2011

Potential Impacts: Hailstorms do not threaten lives to the extent that other natural hazards do, and hailstorms do not typically result in the disruption of critical services, but are among the costliest hazards in terms of property damage. Road vehicles, structures, aircraft, livestock, and crops are most susceptible to hail damage. Ground transport is rendered more dangerous, and can be slowed or temporarily halted. Even small volumes of hail can produce substantial damage to crops. Aviation assets can rapidly sustain damage when exposed to hail. Serious injuries and fatalities are rare, but can occur.

Potential Energy Sector Impacts: *Negligible.* May cause cosmetic or minor to moderate damage to grid components, and may slow or halt regular maintenance activities. Hailstorms may occur concurrently with other atmospheric hazards like thunderstorms, tornadoes, and windstorms, potentially compounding the challenges of response to these hazards.

Hail in Colorado: The state of Colorado lies within the boundaries of “hail alley” and receives the most hail from mid-April through mid-August. According to the Rocky Mountain Insurance Information Association, hail has caused over \$3 billion in insured damage in the past 10 years. The following map shows severe weather reports in Colorado for the year 2011. Each green dot represents a report of hail.

Figure X-5 Severe Hail Reports in Colorado 2011



July 21, 2009. Photo by John Leyba: Denver Post

Summer 2009: The 2009 hail season was one of the costliest seasons for hail damage in Colorado. Three separate incidents combined to produce a total of over \$1.3 billion in insurance claims.

- June 6-15(Denver Metro) \$353.3 million
- July 20 (Denver Metro) \$767.6 million
- July 29 (Pueblo) \$232.8 million

The July 29 storm in Pueblo damaged up to 15,000 cars and 6,000 houses as areas southeast of the city experienced tennis-ball sized hail. The July 20 storm hit the Denver metro area hard, causing nearly \$800 million in damage and disrupting power for 50,000 customers through the night as downed tree limbs

damaged power lines. The image to the left shows Xcel Energy employees removing pressure to the line as a damaged tree leans heavily against a power line.

July 11, 1990: The July 11th hailstorm was the costliest single hailstorm in the state's history. In 2010 dollars, this storm caused \$1.04 billion in damage. Hail as large as baseballs pounded metro Denver and 47 people were injured at Denver's Elitch Garden's amusement park. Hail clogged storm sewers and caused 3-6 feet of flooding in Arvada.

Precipitation

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
US-Regional/State-Regional	Moderate	Regular	Certain	Moderate	63.83

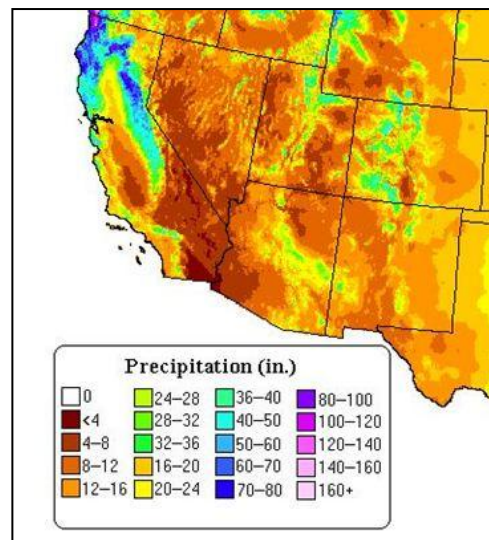
General Summary: Precipitation refers to any form of water that falls on the Earth's surface. Precipitation may take the form of rain, snowfall, sleet, or hail. Colorado is located in a relatively low-precipitation region of the United States, and experiences precipitation to different extents by state region, with the high mountains generally receiving higher snowfall than other regions, but significant potential for snowfall and other precipitation throughout the state.

Potential Impacts: Precipitation levels determine overall water supply throughout Colorado. Heavy snow may directly cause property damage threatening structural integrity and leading to occasional deaths or injuries, and may impact critical services and facilities.

Heavy precipitation may occur in concurrence with other hazards such as thunderstorms and winter weather, or may be a precursor to secondary hazards such as flooding, ice movement, erosion, subsidence, avalanche, landslide, or rock falls. Heavy precipitation can complicate or halt aviation operations in affected areas, and large snowdrifts are capable of derailing or halting rail vehicles. Heavy precipitation can slow or halt road transport, and is a common contributor to road accidents.

Potential Energy Sector Impacts: *Moderate.* Heavy icing can damage and disrupt power infrastructure, and high precipitation conditions may complicate maintenance and response operations.

**Precipitation: Annual Climatology
1971-2000**



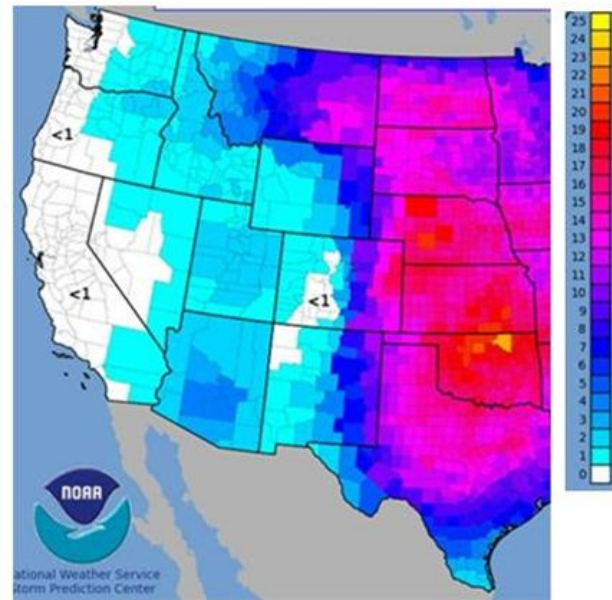
Spatial Climate Analysis Service, Oregon State University; map created Feb 20, 2004

Thunderstorms

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
US-Regional/State-Regional	Severe	Frequent	Certain	Severe	75.41

General Summary: Thunderstorm refers to moving lightning-bearing clouds and cloud systems, which are typically cumulonimbus. Single cell thunderstorms tend to be smaller, are rarely associated with severe weather, and dissipate quickly, but are difficult to forecast due to their rapid and localized development. Multi-cell thunderstorms are composed of multiple single cell storms. Multi-cell thunderstorms are the most frequently occurring storms in most areas, and are generally of moderate severity. Multi-cell and larger thunderstorm systems may advance in a squall line; producing heavy and sustained straight-line winds sometimes classified as derecho events, and may produce moderate tornado activity. Particularly large or severe multi-cell thunderstorms are termed supercells. Supercells are frequently associated with several interrelated atmospheric hazards, all of which can be severe. These include: lightning, straight-line winds/derechos, tornadoes, microbursts, and heavy precipitation often including severe hail and sufficient precipitation volume to cause flash flooding. In Colorado, thunderstorms are seasonally frequent from the Front Range to the eastern plains, and considerably less prevalent in the central and south-central high mountains and west of the continental divide.

Average Number of Annual SPC Severe Thunderstorm Watches per county



Potential Impacts: Thunderstorms are precursors to several types of severe weather including lightning, straight-line winds/derechos, tornadoes, microbursts, and heavy precipitation which can include severe hail and sufficient precipitation volume to cause flash flooding. The damage caused by a thunderstorm is a result of the additional atmospheric hazards associated with them, rather than the storm system itself. In Colorado, flash flooding has posed the greatest hazard of death or injury associated with thunderstorms, followed by lightning, high winds, tornadoes, and hail.

Potential Energy Sector Impacts: *Severe.* Each of the atmospheric hazards associated with thunderstorm activity entail different potential impacts to the energy sector in Colorado. See sections on lightning, windstorms, flooding, tornadoes, and hailstorm for their associated energy sector impacts.

Winter Weather

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
US-Regional/State-Regional	Severe	Frequent	Certain	Severe	75.41

General Summary: Winter weather refers to weather events that include heavy, blowing, or drifting snow, freezing rain/ice storm, and/or extreme cold temperatures. Blizzard refers to winter storms involving wind and blowing snow which severely hinder visibility, but may involve snow that has already fallen rather than new precipitation. Severe winter weather may impact any area of Colorado, with heavy snowfalls and extreme cold temperatures regularly occurring from the high mountains to the Front Range foothills out to the eastern plains.

Potential Impacts: Winter storms may result in heavy drifting snow and icing. Blizzard conditions may severely hinder visibility from ground or air. Heavy precipitation and icing on roadways slows and renders hazardous road travel. In zero visibility, heavy drifting, or heavy icing conditions, motorists are frequently stranded and mobility of emergency response and other critical personnel is constrained. Under some conditions aviation emergency response assets are grounded. Airports may suspend service, stranding planes and passengers. Heavy snow loads may damage structures and collapse roofs, and sustained extreme low temperatures can freeze pipes and cause substantial damage to homes, businesses, and critical facilities. Extreme cold temperatures and deep drifting snow can pose a serious hazard to exposed persons and livestock. Late season heavy snows, icing, and extreme low temperatures can cause significant crop damage. Winter weather can cause and/or compound other hazards and dangerous conditions such as avalanche and flood.



Christmas Blizzard of 1982



Colorado Holiday Blizzards 2006/07
Snowplows on the Highland Bridge
in Denver by Jeff and Cindy Newton

Potential Energy Sector Impacts: *Severe.* Extreme winter weather has caused significant outages and infrastructural damage in the past, and is expected to do so in the future. High winds and heavy icing frequently down transmission and distribution lines, and winter weather conditions can hinder maintenance and emergency response. Geographically widespread damage and difficult response conditions have resulted in localized multi-day outages, with concurrent impacts to critical services and facilities. Winter

weather conditions may both cause and compound the impact of outages: continuity or recovery of aviation, rail, and road transport assets, telecomm, and critical government services may be challenged by electrical outage and extreme weather conditions. Staffing is often hindered, as key personnel must secure transportation to and from worksites. Severe and sustained winter weather conditions may slow delivery of liquid fuels, reducing or eliminating backup generation capability among critical services and sectors in the case of prolonged electrical outage.

Winter Weather in Colorado: Two of the three most recent presidential disaster declarations in Colorado have been for winter weather events. In March 2003 and April 2001 the state of Colorado received federal funds from disaster declarations. The Rocky Mountain Insurance Information Association estimates that the March 2003 storm was the costliest winter weather storm in Colorado; with a price tag of \$93 million. The following table describes the four costliest winter weather events in Colorado’s history.

Table X-13 Costliest Winter Storms in Colorado

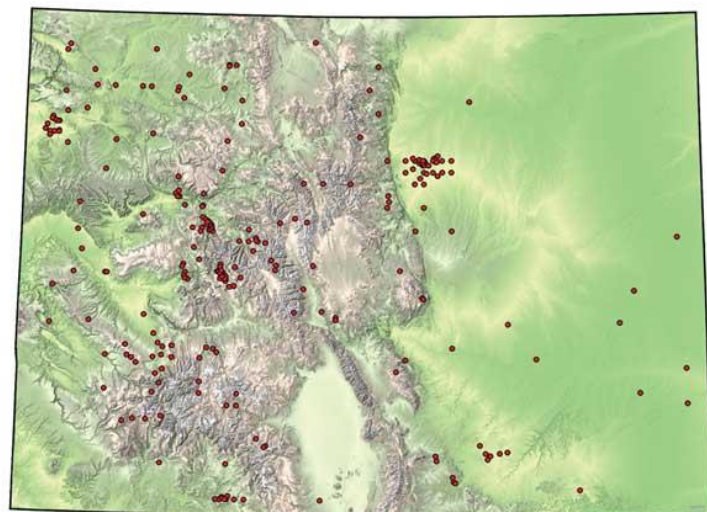
Date	Cost	Description
December 20-22 & 27-29, 2006	Total cost unknown: Frontier Airlines lost \$14 million, United Airlines lost \$30 millions, and the closure of I-70 may have cost the state up to \$600,000 per hour.	Back to back blizzards struck the Front Range during ten of the busiest travel days of the year. The Denver International Airport was closed for two days during the first system. A second system moved through after Christmas and dropped more snow on the Front Range while stalling over Southeast Colorado where the snow continued and wind speeds sped up to 30-50 mph. Over 15,000 head of cattle were lost and the National Guard was called in to drop hay bales to keep more from dying. Power outages lasted for up to two weeks in some places.
March 17-20, 2003	\$93.3 million	87.5” of snow was recorded in Rollinsville. Many roofs were destroyed under the heavy snow and power lines were damaged due to broken tree limbs.
October 24-25, 1997	\$10.5 million	Extended snowfall rates of 1-2 inches per hour, winds of 30-40 mph, and a low of 3 degrees on October 26 th with a final tally of 2-4 feet of snow in the foothills and 14-31 inches along the Denver metro. The storm claimed four lives and stranded 4,000 motorists on Pena Boulevard.
September 20, 1995	\$6.4 million	Wet snow dropped thousands of tree branches and downed power lines leaving 100,000 people in Boulder without power. 4-8 inches of snow fell in Denver during this late summer storm.
December 22-26, 1982	\$4.9 million	4-10 foot snowdrifts covered the Denver Metro area. Travelers were stranded at the airport while employees and shoppers were stranded at malls and shopping centers. For the first time in history, every surrounding highway was closed.

Earthquake

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
State-Regional	Catastrophic	Rare	Rare	Catastrophic	63.26

General Summary: Earthquake refers to vibrations and displacements produced by movement of seismic faults, or less frequently, by volcanic, magmatic, or human activity. Earthquake magnitude refers to total energy released, while earthquake intensity refers to specific impacts within a defined area. The Richter Scale and Modified Mercalli Scale are commonly used to classify earthquake magnitude and intensity, respectively. Earthquakes may be preceded by foreshocks, or may occur with little or no warning. Earthquakes are frequently followed by aftershocks of somewhat lesser magnitude. Earthquakes are generally triggered by seismic activity, but human activities like mining, liquid fuels extraction, fluid injection, and reservoir impoundment can be contributing or causal factors. Proximity to the epicenter is correlated with increased intensity, but impacts can be unevenly distributed, with some areas further from the epicenter more heavily impacted than other areas closer to the epicenter. Earthquakes with significant ($X > 3.0$ Richter) destructive potential are most probable in areas of the central and southern high mountains and west of the continental divide, with the eastern edge of the San Luis Valley at the base of the Sangre de Cristo range, and the Sawatch fault at the eastern margins of the Sawatch Range having the highest potential for activity. Nevertheless, earthquakes may occur anywhere in the state.

The Denver metro area and Front Range foothills have occasionally been impacted by relatively minor ($X < 3.0$ Richter) earthquakes, but could potentially experience infrequent but dangerous and costly events of 6.5 magnitude in or near metropolitan areas. While relatively low-probability, an earthquake centered on one of the faults along the Front Range metropolitan area could potentially result in billions of dollars in damage, substantial infrastructural disruption, and hundreds of fatalities. The eastern plains are rarely impacted, and virtually no earthquake activity occurs in the northeastern quarter of the state.

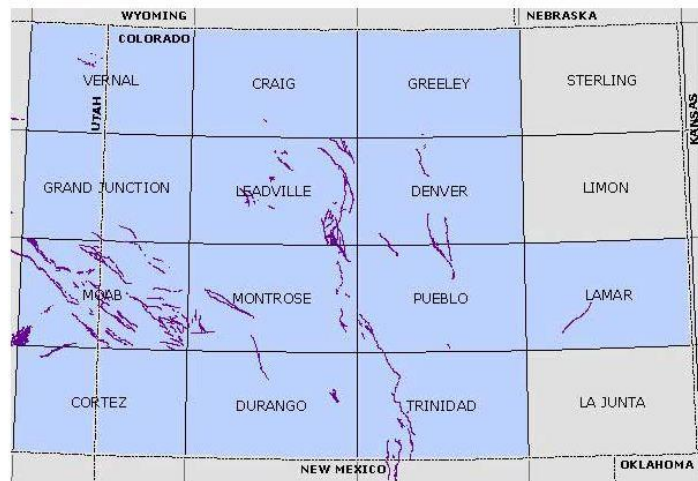


Colorado Geological Society
Earthquakes in Colorado: 1867-1996

Potential Impacts: Shaking, vibration, ground rupture, and soil liquefaction are primary effects. Local geological, geostructural, and geographic features can produce disproportionately powerful effects termed local amplification. Ground shake is a hazard for all rigid constructions including residential, commercial, industrial, and government properties. Ground rupture can pose a severe risk to large engineering structures such as dams, bridges, aqueducts and water pipelines, liquid fuels pipelines, mines, generating stations, and similar structures. Depending on other geologic factors, soil liquefaction may occur, and this can pose a severe hazard when it occurs beneath large and populated structures. Airport runways can be compromised. Earthquakes may be a primary hazard which causes or compounds secondary hazards. For example, earthquakes have caused massive rockslides into rivers and reservoirs, causing floods, dam failures, and overtopping. Earthquakes may be causal, contributing, or aggravating factors to tsunamis, landslides, rock falls, ice falls, avalanches, mudslides, fires, flooding, and soil liquefaction. Each of these secondary hazards are likewise associated with a series of unique impacts.

Potential Energy Sector Impacts: *Catastrophic.* While the probability of a severe or catastrophic earthquake is lower in Colorado than in some western states, the potential for a severe or catastrophic quake does exist in some areas. Impacts within Colorado would likely be regional, with defined areas of moderate, severe, or catastrophic impact, surrounded by areas of progressively lower impact.

Any un-reinforced or unmitigated energy sector asset, component, or facility in affected areas could be damaged or destroyed. Transmission and distribution lines may be downed, and substations damaged or disabled. Generating stations and other facilities could sustain substantial damage, dams and hydroelectric facilities could be damaged, ruptured, or overtopped due to rock fall or secondary hydrologic activity. Pipelines and liquid fuels storage tanks could rupture, leading to fuel loss, ecological damage, and urban fires or wildfires. Situation reporting and damage assessment may be slowed by telecommunications disruption, and access for response and recovery may be hindered by damage to fleet vehicles, roadways, or aviation assets and facilities.

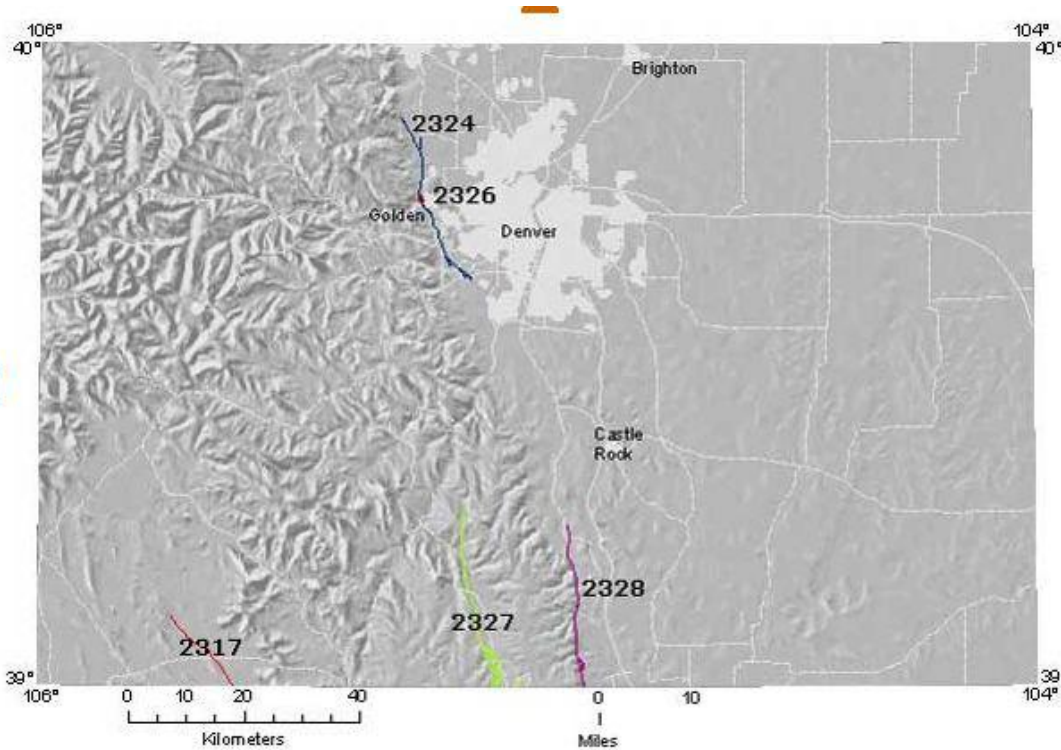


USGS & Cooperator Colorado Geological Society
[Quaternary Fault Lines in Colorado](#)
 Fault lines that have evidenced movement in the past 1.6 million years

Earthquakes in Colorado: The first earthquake to cause damage in Colorado occurred on November 7, 1882. It measured in at 6.6 on the Richter scale and was felt as far east as Salina, KS and as far west as Salt Lake City, UT. In Denver electricity was lost when an iron bolt that connected an engine-driving pulley was broken. The costliest earthquake in Colorado occurred on August 9, 1967 when a magnitude 5.3 earthquake caused \$1million in damage to the Denver Metro area. This particular event was the result of a deep injection of liquid waste at the Rocky Mountain Arsenal. Throughout the 1960’s, hundreds of minor tremors and earthquakes occurred in and near the Rocky Mountain Arsenal.

More recently, on April 22, 2011, a 5.2 magnitude earthquake struck Las Animas County in southern Colorado causing over \$300,000 in damage. Most of the damage occurred to older structures that were constructed of materials that were not designed for earthquake-prone regions (stucco, adobe, and loose brick).

Figure X-6 Denver Metro Area Quaternary Faults



Source: USGS & Cooperator Colorado Geological Society

- *2324 Golden Fault
- *2326 Graben Fault near Golden
- *2328 Rampart Range Fault
- *2327 Ute Pass Fault Zone
- *2317 East-Side Chase Gulch Fault

Erosion and Deposition

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
State-Regional/Localized	Slight	Regular	Certain	Slight	47.57

General Summary: Erosion refers to a naturally occurring process by which material is removed from the Earth's surface. Deposition refers to the depositing or settling of these materials in a new location. The geologic and atmospheric erosive processes that cause initial erosion, also typically increase the rate of subsequent erosion, causing an acceleration of erosion and deposition over time. In Colorado, erosion is usually initiated by water or wind flows. Erosion related to streamflows is termed riverine erosion. Human activities like agriculture and construction which involve rearrangement of drainage channels, irrigation, exposure of earth or removal of vegetation, can contribute to erosion. Heavy rain and rapid streamflow, and heavy winds can contribute to erosion. Floodwaters can rapidly carry large volumes of rock and earth from one location and deposit them elsewhere. Dry and exposed agricultural areas as well as fire burn areas are particularly susceptible to wind erosion. Softer and drier earth materials like sand and silt are most susceptible, while hard granites and solid rock formations are less susceptible. Onset is generally gradual, but sudden emergence of contributory conditions like swift water flows through diverted drainage culverts may rapidly erode drainage channels and earth berms, resulting in road washouts and other rapidly-developing damage. Highly engineered structures like bridges and roadways can be structurally undermined by the erosion of earth foundation, and seriously damaged or destroyed.

Potential Impacts: Riverine erosion can cause land loss, marine transportation problems, and harbor and waterway sedimentation. Agricultural runoff can contribute to reduction of water quality and ecological damage. Wind erosion contributes to topsoil loss, root exposure, and other agricultural problems. Erosion can contribute to dust storms, which hinder ground transportation and increase stresses on motorized vehicles and agricultural and industrial machinery. Deposition of dust particles on mountain snowpack can result in unseasonably early snowmelt.



Deposition downstream from an erosion zone after the Buffalo Creek Fire in Pike National Forest

Potential Energy Sector Impacts: *Slight.* Wind and water erosion can contribute to isolated infrastructure damage or failure, but are unlikely to produce serious simultaneous impacts over a significant geographic area. Planning, mitigation, and monitoring efforts can reduce the probability of significant impacts to energy infrastructure and assets. Rapid erosion and deposition can follow other atmospheric or hydrologic hazards like windstorms and flooding, and should be considered among possible byproducts of these hazards.

Erosion and Deposition in Colorado: Two months after the May 1996 Buffalo Creek Fire in Pike National Forest, flooding and erosion transported 30 times the annual rate of coarse sediment into the Strontia Springs Reservoir. At the time, the Strontia Springs Reservoir supplied the city of Denver with 75% of its drinking water. The Denver Water Department spent years cleaning up the reservoir after water quality tests proved that the burned materials and sediment were degrading water quality. In 2010, the Waterton Canyon Recreation Area was closed and the Strontia Reservoir dredged to remove the remaining sediment. A 9 mile long pipeline was installed to carry the hundreds of thousands of tons of sediment down to the mouth of Waterton Canyon. In April 2012, nearly 16 years after the Buffalo Creek Fire and a decade after the Hayman Fire, the 75 ton dredge was removed and the project was finally completed.

In 1998, Pikes Peak Highway was at the center of a lawsuit between the Sierra Club and the City of Colorado Springs and the USDA Forest Service. The unpaved highway was built without proper water control structures. Storm water eroded the road and carried thousands of tons of gravel and sediment down to natural watersheds every year. Over time, hundreds of gullies formed and increased the rate of erosion. The lawsuit was settled when the City of Colorado Springs and the US Forest Service agreed to pave the upper 12 miles of road at a cost of \$17-\$20 million. Paving began in 2001 and is scheduled to be completed by the end of 2012.



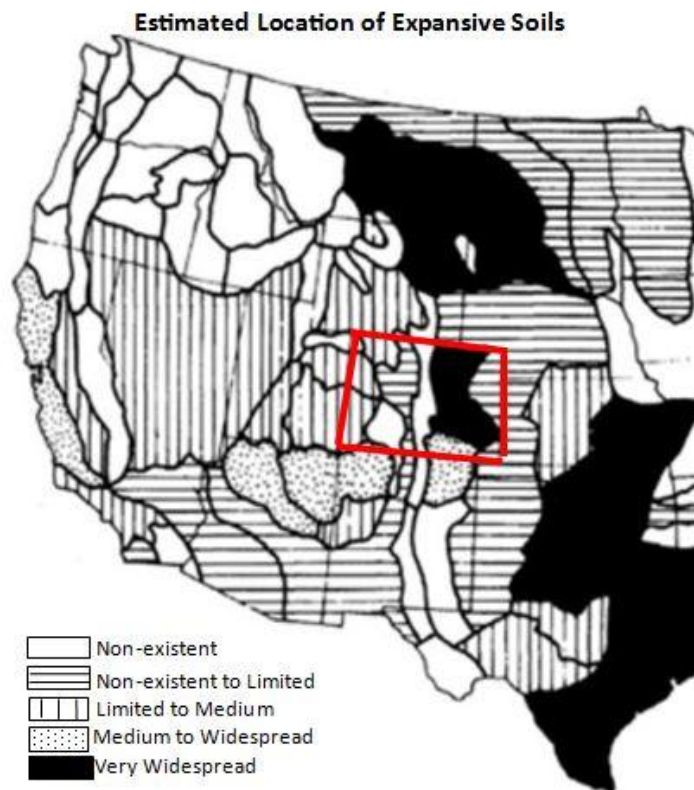
The Pikes Peak Watershed Erosion Control and Restoration Project: removing over 270 cubic yards of sediment from the Glen Cove wetland area. Image from the Rocky Mountain Field Institute

Expansive Soils

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
State-Regional/Localized	Moderate	Periodic	Very Likely	Slight	43.82

General Summary: Expansive soils refer to soils and underground rock which expand or contract in volume due to the introduction or removal of water and pressure. Soil expansion may be caused by natural processes like droughts and precipitation, or can be caused by construction and other human activities involving excavation and the intentional or unintentional introduction of water to previously dry subsurface rocks and soils. Likewise, sub-surface bedrock may expand and heave, causing similar and sometimes more severe damage.

The sub-surface hydrologic and geologic processes that contribute to soil expansion and heaving bedrock in particular can be challenging to predict without careful survey. Certain types of soils and underground rock are more susceptible to expansion upon the introduction of water. Soils high in certain clay particles are particularly susceptible, and may expand by more than 10% by volume upon the introduction of water.



A 1972 map predicting the location of expansive soils

Potential Impacts: While they very rarely threaten life safety, expansive soils are a regular cause of property and infrastructure damage in the United States. Expansion can exert substantial vertical or shearing force on foundations and underground structures. Once expanded, soils may or may not revert to original volume upon drying. All types of residential, commercial, industrial, or government construction may be impacted in susceptible areas, with impacts ranging from severe damage to subterranean structures like basements and foundations, heaving or shearing of roads and other highway structures, and disruption of pipelines,

underground drainage, sewage lines, utility lines, utility tunnels, steam tunnels, and subterranean mining and storage facilities.

Potential Energy Sector Impacts: *Slight.* While soil expansion can present with a moderately rapid onset, and can cause severe structural damage in some cases, it can often be mitigated or prevented with sound surveying, construction, and maintenance practices. Energy assets and facilities located in susceptible areas may be seriously impacted and subterranean infrastructure like pipelines and utility tunnels may be particularly impacted. However, because soil expansion very rarely involves simultaneous severe impacts over a wide geographic area, potential impacts to energy assets are relatively infrequent, isolated, and often preventable.

Expansive Soils in Colorado: Soil expansion may occur anywhere in Colorado, but portions of Crowley, Elbert, Lincoln, Moffat, and Routt counties have soils particularly conducive to expansion. Bedrock heaving is generally limited to areas of the central Front Range, particularly effecting Douglas and Jefferson counties.



Expanding soils buckle many roads in Colorado. Image from the Colorado Geological Society

According to the Colorado Geologic Society, expansive or swelling soils may be one of Colorado's most significant geologic hazards. Damage from expanding soils costs billions of dollars world-wide each year, more than all other natural disasters combined. The map below demonstrates just how widespread this hazard is in Colorado. Most of Colorado is prone to swelling soils of a slight, moderate or abundant degree. In the past, expansive soils have damaged structures at Colorado State University in Pueblo and prevented the construction of a State Prison in Fremont, Colorado. This phenomenon has caused damage to countless roads and structures throughout the state.

Figure X-7 Expansive Soils Map



Map I-1940 in the USGS Miscellaneous Investigations Series

Red:
>50% of these areas are underlain by soils with abundant clay and swelling potential

Blue:
<50% of these areas are underlain by soils with abundant clay and swelling potential

Light Green:
<50% of these areas are underlain by soils with slight to moderate swelling potential

Olive Green:
These areas are underlain by soils with little to no swelling potential

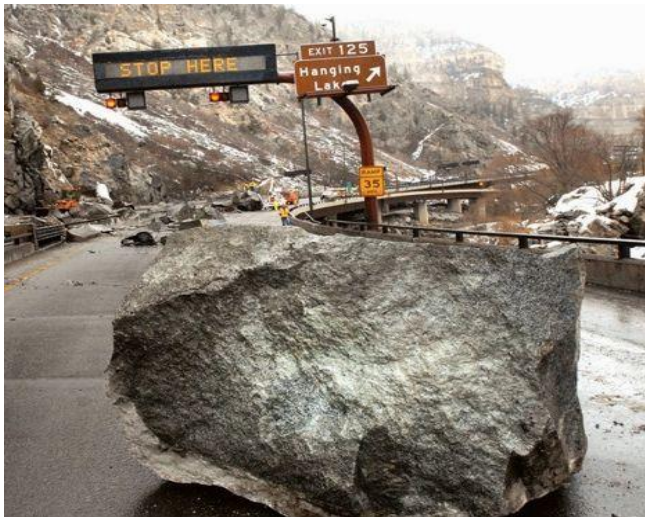
Yellow:
Insufficient data

Source: *Swelling Clays Map of the Conterminous United State* by W. Olive, A. Chleborad, C. Frahme, J Shlocker, R. Schneider and R. Schuster, 1989.

Landslides/Mudflows/Rock falls

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
State-Regional/Localized	Moderate	Periodic	Moderately Likely	Moderate	49.16

General Summary: Landslide refers to the down slope movement of geologic materials and surface debris. Mudflow refers to a combination of water and soil materials flowing downslope along ravines, canyons, gulches, and other water-eroded geologic features. Rockfall refers to the falling of rock masses down cliffs and other steep slopes. In Colorado, most landslide, mudflow, and rockfall activity occurs along the Front Range, central mountains, and Western Slope, but may occur in any part of the state with significant grades and elevation changes. Landslides are the product of an increase in driving forces and pressures facilitating material breakaway and down slope movement, and/or a decrease in the resisting forces that prevent materials from breaking away and moving down slope. Consistent precipitation and the freeze/thaw cycle are typical contributing factors, but seismic activity can also facilitate slide behavior. Human activity is also an occasional contributor to slides, with construction, hydrologic engineering, mining, blasting, and any other activity which mimics seismic or water-erosive activity being occasional potentiators of slide activity. Slide activity occurs sporadically and can be difficult to forecast. Slide activity may be so slow in onset as to be almost undetectable without careful observation, or may develop into a major and irreversible hazard with extreme rapidity.



March 8, 2010: rockslide on I-70 at exit 125 for Hanging Lake. Image from CDOT

Potential Impacts: General impacts are typically localized but can be very severe. Structures and improvements located on slope can be carried along with other slide debris, and masses of slide material can produce forces sufficient to carry away any unsecured objects including large vehicles, block, damage, or destroy roadways, and strip structures from foundations. The fanning-out of slide material at the slide's termination can result in expensive and time-consuming cleanup, particularly in cases of roadway and utility disruption. In Colorado, slide activity rarely results in death or injury, but deaths and serious injuries have occurred.

Potential Energy Sector Impacts: *Moderate.* Energy sector assets and activity can be threatened by slide activity, and can also be a contributing factor to slide activity in rare cases.

Utility conduits and pipelines may be located in areas with high slide potential, and the foundation work and excavation to emplace these infrastructural assets can combine with other factors like precipitation, drainage, and seismic tremors to produce slide activity. More often, natural slide activity can damage or destroy energy assets located on slopes or at the slide's termination areas down slope. Assets potentially affected include conduits, utility lines, poles, access roads, and substations located on slopes and in termination zones. Though slide activity is capable of significant infrastructural damage, it is typically localized, and impacts major assets relatively infrequently.

Slide Activity in Colorado: Shortly after midnight on March 8, 2010 a landslide descended onto Interstate 70 near Glenwood Springs. Over 20 boulders between 3 and 20 feet in diameter punched holes into the pavement and caused over \$2 million in damage. No one was injured or killed during the slide. This is not the first time that a landslide has struck the Glenwood Springs area. In 1994, the South Canyon fire took the lives of 14 firefighters and scorched the hillside along Storm King Mountain. Two months later, heavy rains caused landslides along a 3 mile stretch of Interstate 70. At least 30 cars were damaged during this event and transportation along the I-70 corridor was brought to a standstill. In 2002, the Coal Seam fire burned 12,228 acres of steep hillside near Glenwood Springs. Once again, debris flow from heavy rain and the weakened slope caused landslides in this region. Figure X-8 shows the outlines of both the Coal Seam Fire and South Canyon Fire with the resulting landslides/debris flows. These debris-flow paths are in red with Interstate 70 travelling parallel to the Colorado River.



The 1994 Glenwood Springs debris flow along I-70
Photo by Jim Scheidt, Bureau of Land Management

Figure X-8 Debris-Flow Response of Basins Burned by the 2002 Coal Seam and Missionary Ridge Fires

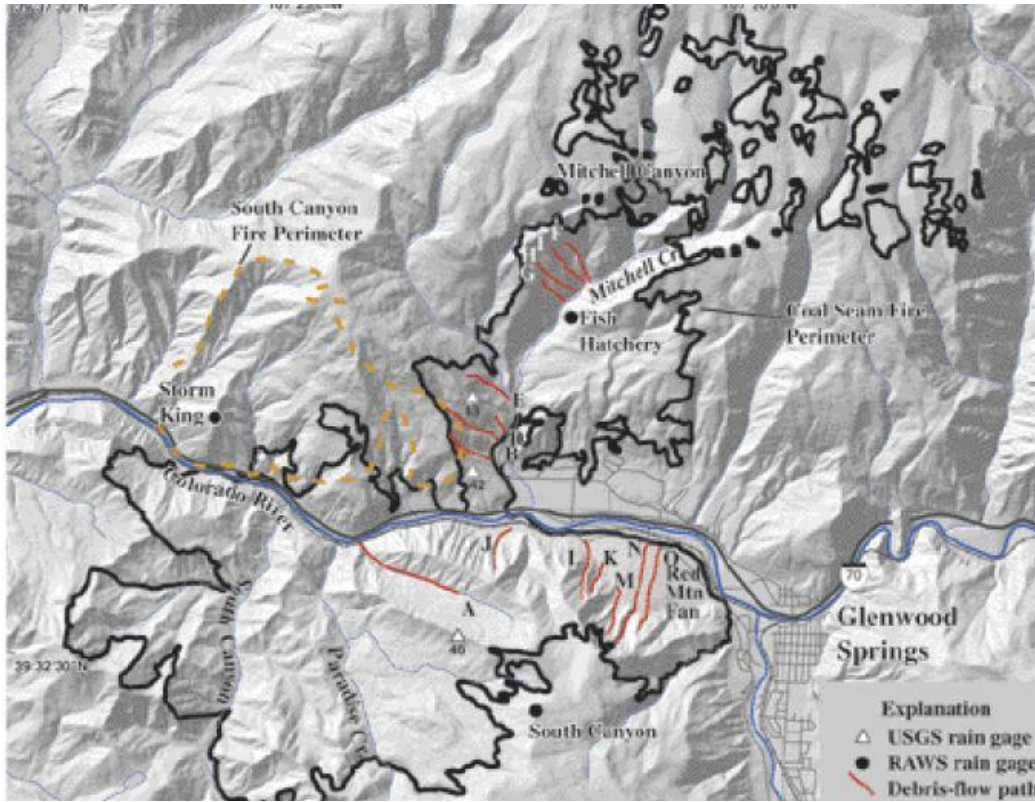


Image from "Debris-Flow Response of Basins Burned by the 2002 Coal Seam and Missionary Ridge Fires, Colorado" by Susan H. Cannon, Joseph E. Gartner et al.

Figure X-9 The Anatomy of a Landslide

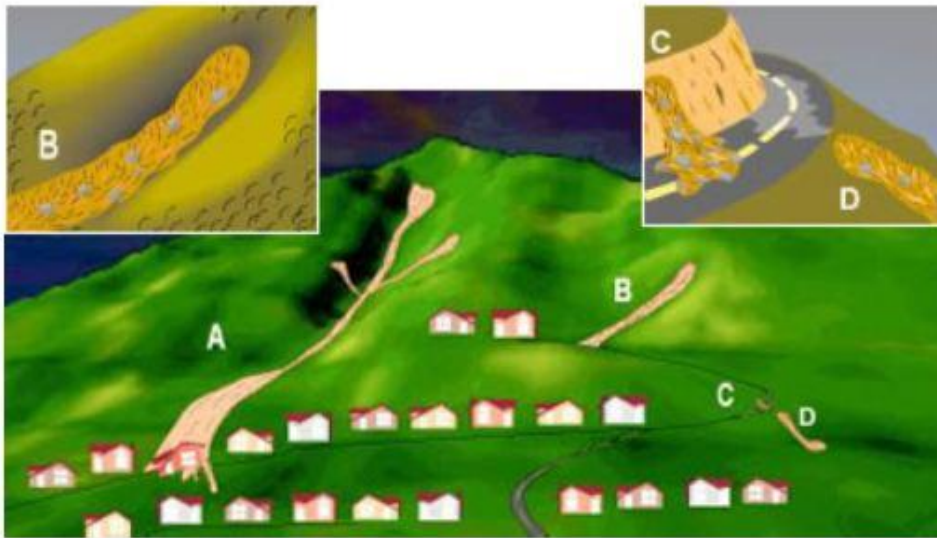


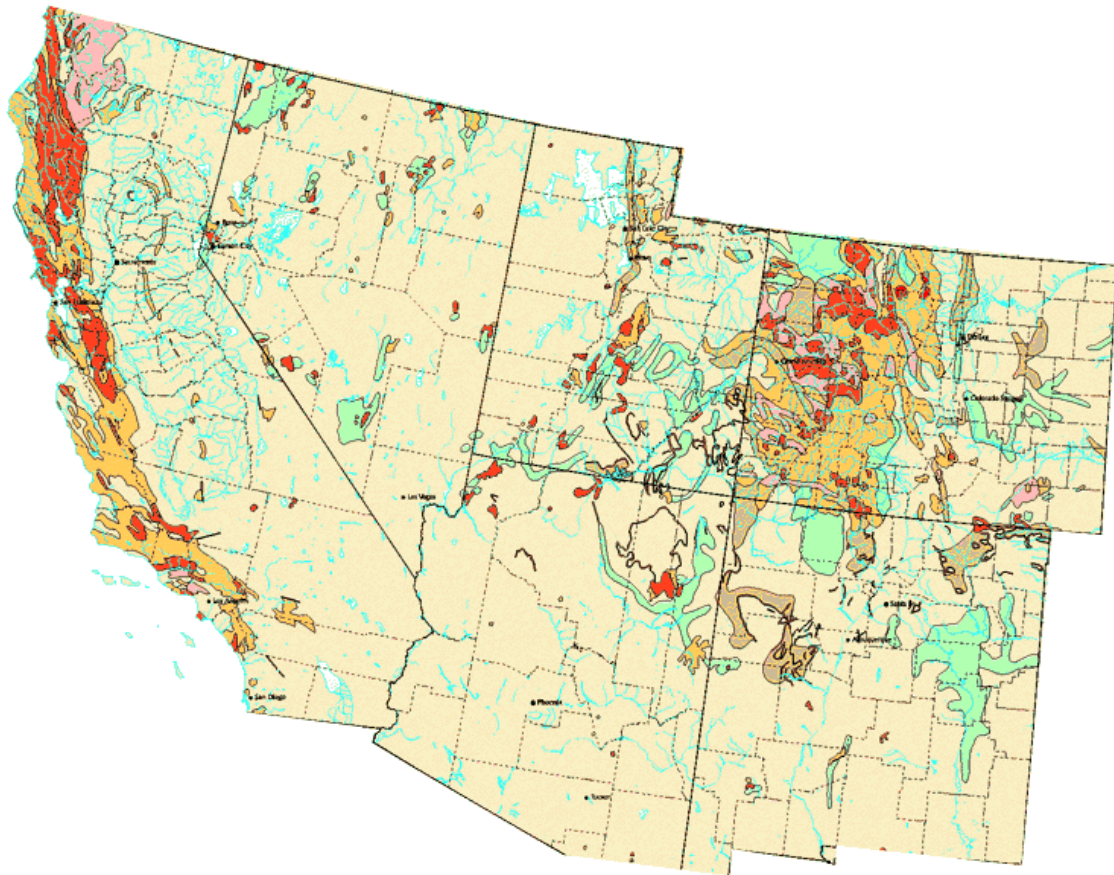
Illustration provided by United States Geological Survey Fact Sheet 176-97

Canyon bottoms, stream flows, and any areas near the outlet of a canyon are particularly prone to landslides. Multiple debris flows that start higher up in a canyon may funnel into the main canyon outlet.

- Debris flows commonly begin in swales, or depressions, along steep slopes.
- Road cuts or other altered areas of slope are also particularly prone to debris flows. These types of debris flow are common during rain storms and can occur easily and more often than debris flows from natural slopes.
- Areas where surface runoff is channeled are common sites of landslides and other debris flow

Wildfire and heavy rain is not the only cause of debris flows in the state of Colorado. On the outskirts of Grand Junction, the construction of suburban homes reactivated an old landslide and caused extensive damage to at least 10 homes. Utilities below the perimeter of the slide were also at risk. The project and a number of new homes had to be abandoned. This man-made landslide could have been prevented with the use of available geotechnical data; aerial photo analysis showed that evidence of the previous landslide existed on the site as early as 1954.

Figure X-10 US Geological Society: Landslide Overview Map of Conterminous United States



Landslide Incidence

- Low (less than 1.5% of area involved)
- Moderate (1.5%-15% of area involved)
- High (greater than 15% of area involved)

Landslide Susceptibility/Incidence

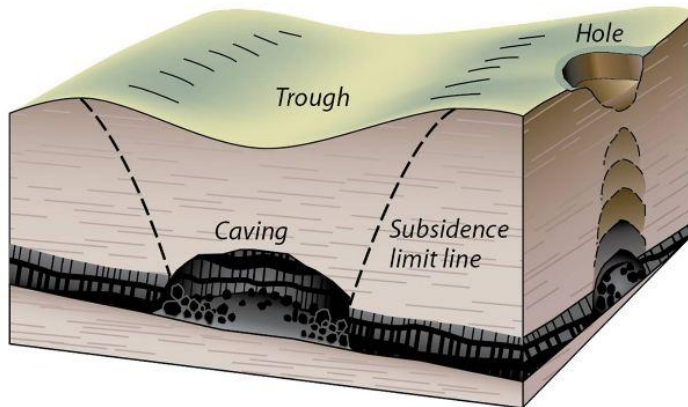
- Moderate susceptibility/low incidence
- High susceptibility/low incidence
- High susceptibility/moderate incidence

Subsidence

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
Localized	Moderate	Periodic	Certain	Slight	43.49

General Summary:

Subsidence refers to the sinking of surface land over natural or human-made subterranean voids. Subterranean voids may be created by a variety of human activities including the pumping of groundwater or petroleum, underground mining, and draining. Natural causes of voids include sinkhole development, sediment compaction, collapsing and settling soils, permafrost melting, and other geologic and hydrologic phenomena. Onset may be very rapid, or may develop slowly over a period of years.



Subsidence caused by mining. Image from the Colorado Geological Survey

Onset may be very rapid, or may develop slowly over a period of years.

In Colorado, many of the most serious subsidence have been over mining works, and subsidence caused by soil collapse tends to occur in drier areas as groundwater and seepage causes destabilizing hydro-compaction of previously dry soils. Subsidence can produce serious damage or destruction of structures, roadways, and utility infrastructure. Conditions conducive to subsidence exist over much of Colorado, with the Front Range, Western Slope, and high mountains around Eagle County being most often impacted. Undermined areas are at particular risk, but subsidence potential can be assessed in many potential problem areas.

Potential Impacts: Subsidence can rapidly or slowly displace underground or surface structures several feet. Large ground displacements can damage or destroy roads and other infrastructure, and disrupt or re-route surface drainage channels. Displacements may be filled, only to sink further below surface as the void continues to develop. Damage to subterranean and surface structures may range from minor damage to foundations and utility lines, to total loss.

Potential Energy Sector Impacts: *Slight.* Energy sector activities like mining and liquid fuels extraction can contribute to subsidence conditions. Impacts to service roads can limit accessibility for maintenance and emergency response activities. Pipelines, electrical

transmission lines, substations, and some generating facilities may be moderately to severely damaged, but these impacts are typically isolated and localized when they occur.

Subsidence in Colorado: In response to rapid population growth in the area, the Colorado Geological Survey and USGS Geologic Mapping Team mapped the Interstate 70 corridor and determined that soil stability problems occur all along the region. The hydro-compaction of low-density sediments like sandy silt can cause subsidence as the soil becomes saturated with and forms large, destructive cavities. The following image shows a sinkhole near Carbondale, Colorado where the hydro-compaction of deposits and underground piping from water erosion caused a large void about 80 feet across and 10 feet deep.



A large sinkhole at the Colorado Mountain College.
Image from the Colorado Geological Survey

Natural Subsidence

February 2003, Colorado Mountain College, Roaring Fork Campus near Spring Valley: The Colorado Mountain College physical plant staff responded to a report of a 25 foot diameter sinkhole opening up on the campus soccer field. Employees filled the hole with road waste but returned to a reopened sinkhole at 35 feet in diameter. An investigation revealed a layer of Eagle Valley Evaporite at 65 feet below the surface of the sinkhole.

Coal Mine Subsidence

December 2008, Erie County, Colorado: A 50 foot diameter/30 foot deep subsidence hole was reported in December 2008 from a field west of Erie slated for future residential development. The mine map used to determine the location for this development was incorrect and another small sinkhole soon opened up west of the original. Both holes were filled by the Abandoned Mines Program.

Colorado School of Mines 2005

The Colorado School of Mines in Golden, Colorado has a number of subsidence issues related to abandoned mines. Street damage occurred in 2005 near sorority houses above the athletic fields and a water main rupture made the situation worse.



A buckling road in Golden, Colorado; photo by TC Wait

Solar Weather/Geomagnetic Storm

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
National/US-Regional	Moderate	Rare	Rare	Catastrophic	64.76

General Summary: Geomagnetic Storm (GMS) refers to temporary disturbances or disruptions in the interplanetary medium with impacts on Earth's magnetosphere. These disturbances are produced by fluctuations in solar wind and other solar weather phenomena such as Coronal Mass Ejections (CMEs). As a geologically active planet, the Earth's rotating core of heavy metals produces a magnetic field that shields the atmosphere and surface of the Earth from charged particles produced by the sun. Spikes in solar output can transfer an increased volume of energy into Earth's magnetosphere, resulting in higher radiation absorption, disruption of communications between surface radio and microwave receivers and orbital platforms, disruption of some types of high frequency surface radio communication, damage to orbiting satellites, damage to electrical transmission, generation, and switching equipment, and damage to pipelines, among other effects. Geomagnetic storms powerful enough to cause substantial disturbances to telecommunications and energy sector operations are infrequent, but are more likely during peak solar cycle.

Potential Impacts: Though geomagnetic storms can produce dangerous radiation levels to humans located in orbit or beyond Earth orbit, they do not directly impact life safety on the surface of the Earth. Nevertheless, geomagnetic storms can produce substantial impacts to critical infrastructure if mitigative actions and procedures are not implemented prior to the event. Temporary impacts to the ionosphere can result in disruption to radio broadcast systems which 'bounce' signals off the ionosphere back to surface receivers. Traditional television and commercial radio are not usually disrupted, but high frequency aviation, shortwave, and marine bands, as well as amateur radio bands below 30 MHz can be disrupted. Military over-the-horizon radar systems, as well as submarine communications and tracking systems, can be rendered ineffective by radio clutter. Long-haul telephone lines and non-fiber-optic undersea cables can be impacted. Satellite-based navigation systems like GPS can be adversely impacted, and mitigative measures like Receiver Autonomous Integrity Monitoring (RAIM) may be only marginally effective in maintaining GPS capability during a major GMS event. Satellites may sustain direct damage to components, or may experience degradations in orbit necessitating boosting to avoid atmospheric re-entry and burn up. Satellite-based communications and imaging systems can be disrupted, resulting in blackout of all satellite-based communications during the event.

Potential Energy Sector Impacts: *Catastrophic.* The magnetic fields produced by major GMS events are sufficient to produce geomagnetically induced currents (GIC) in conductors located at

or beneath Earth's surface. Operators of long electrical transmission lines are at particular risk, as longer lines are better able to conduct geomagnetic current. Particularly vulnerable long-line operators are located in North America, China, and Australia. GIC can damage generators and transformers by producing core saturation, performance constraints, coil heating, and the tripping of safety devices. Cascade failures of grid components have been produced by past GMS events, resulting in major regional outages. Preventive and mitigative measures such as transformer disconnection, temporary blackouts, transformer neutral grounding, series compensation, and FACTS devices do exist, but must be implemented prior to the event. GIC can also impact pipeline operations. Pipeline flow meters can receive inaccurate information, and corrosion rates can increase rapidly. Attempts by pipeline engineers to balance for the geomagnetically induced current can be counterproductive if monitoring equipment is already receiving inaccurate information. Though most minor GMS events produce no major electrical outages, and serious outages have typically been limited to single geographic regions during past events, a major GMS event could produce widespread damage to critical telecommunications and energy infrastructure in multiple countries or energy markets simultaneously. Depending on countries impacted, supply chain inadequacies and logistical challenges could elevate the impacts of a major GMS event from *Catastrophic* to *Catastrophic-Systemic*. For additional information on GMS, see Book 3 - Risk and Vulnerability Assessment in the Exercises subsection, under Inter-State Exercise – Geomagnetic Storm.

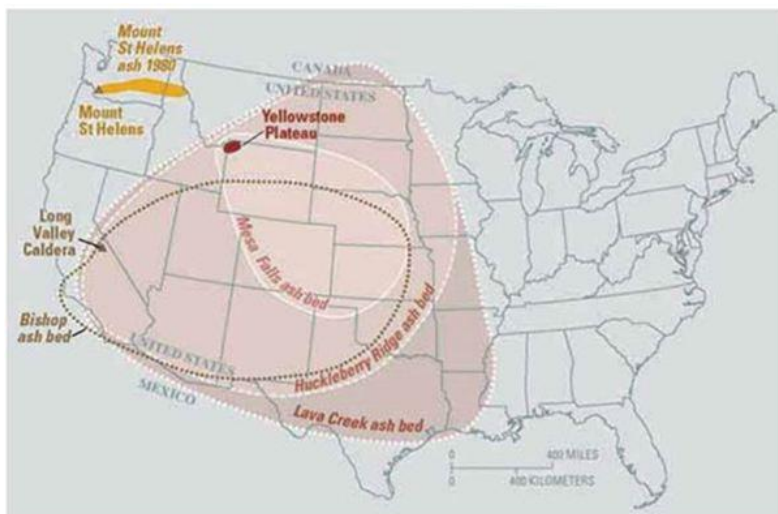
Volcanic Activity

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
Global/National/US-Regional	Catastrophic	Extremely Rare	Extremely Rare	Catastrophic-Systemic	80.00

General Summary: Volcanic activity refers to geologic activity resulting in ejection of subterranean Earth materials onto the Earth's surface and into the atmosphere. Ruptures in the Earth's surface which allow the escape of hot magma, volcanic ash, and gases, are commonly known as volcanoes. Depending on location and magnitude, volcanic eruptions may produce a variety of localized and generalized secondary hazards. Pre-and post-eruption hazards may include earthquakes, fumerole formation, and other seismic disruptions. Localized hazards resulting from eruption may include lava flow, pyroclastic flows, and lahars. Volcanically-induced atmospheric hazards may include ejection of aerosolized ash into the atmosphere, and accompanying climatic and environmental impacts such as ashfall, acid rain, and temporary (X<10 years) global climate change. The onset of volcanic activity, particularly for long-dormant volcanoes, can be difficult to forecast. Colorado currently has no volcanoes classified as active by the US Geological Survey, but like most of the mountain and plains states east of the continental divide, can be impacted by potential supervolcanic activity originating in the Yellowstone Caldera. Though the potential for supervolcanic activity at Yellowstone is notable for its potentially devastating regional and international impacts, the probability of such activity in any given year is calculated at 0.00014%, rendering supervolcanic activity a high-impact low-probability event.

Potential Impacts: Localized hazards like lava flows, pyroclastic flows, and lahars tend to trace local geography, flowing from their points of origin to lower ground. While lava flows do not often pose major threats to life safety due to their limited geographic range and slow movement - they rarely exceed speeds of 40 miles per hour - and can completely destroy all dwellings and infrastructure in their path. Pyroclastic flows are currents of superheated volcanic

Historical Yellowstone Caldera Ash-Fall Ranges

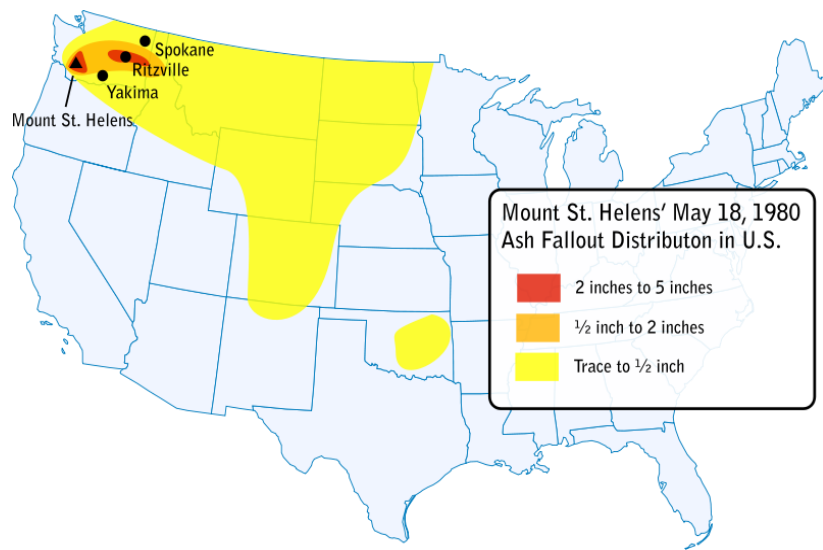


USGS: <http://pubs.usgs.gov/fs/2005/3024/>

gases capable of traveling downslope at speeds up to 450 miles per hour, posing an extreme danger to life and property in its path. Lahars are currents of debris-laden pyroclastic material, mud, and water. This flowing material is fluid while in motion, but gains the consistency of concrete once settled. Lahars have been observed traveling at speeds exceeding 60 miles per hour, and typically cause total destruction to impacted areas. Atmospheric dispersion of ash and its accompanying impacts are the volcanic hazards with widest geographic distribution by far, and ash-related impacts are the most likely to affect Colorado. Ashfall can produce crop damage and water quality degradation. Ash deposits can coat road and runway surfaces, which must be cleared for safe usage. Ash ejected into the stratosphere can disrupt aviation operations, particularly jet transport. Eruptions that exceed magnitude 7.0 on the Volcano Explosive Index (VEI) can produce "Volcanic Winter," a temporary global climate change potentially resulting in regional or global crop failure and other environmental disruptions.

Potential Energy Sector Impacts: *Catastrophic-Systemic.* Any energy infrastructure, assets, or facilities in the path of lava flows, pyroclastic flows, or lahars, are expected to be a total loss. Exposure of infrastructure to these hazards is minimal in most states. In Colorado, vulnerability to these localized volcanic impacts is virtually non-existent. However, depending on volume of ejected ash and environmental conditions, ashfall may pose a particular hazard to electrical infrastructure. Dry ash, even in substantial quantities, tends to cause only minor disruptions to electrical infrastructure, though it can cause overheating and other air quality problems for ventilated and air-cooled equipment in sufficient quantity, can damage or disable surface vehicles and aviation assets, and can result in roof collapse. Heavy winds and rain can wash away much ash, counteracting many of the impacts of ashfall. However, mild precipitation or high humidity conditions can aggravate the impacts of ashfall to electrical infrastructure, as mild precipitation merely wets the ash and increases its weight and electrical conductivity, without physically washing it from components. Transmission lines and substation insulators coated with wet ash may experience flashover, which can cause component damage. Wet ash is heavy, and can cause line breakage, pole collapse, roof collapse, or vegetation collapse that impacts lines and equipment. Telecommunications infrastructure appears to be particularly resilient to ashfall, and telecommunications services may experience fewer disruptions than electrical infrastructure. While the potential for a major Yellowstone eruption resulting in large scale ashfall in

in large scale ashfall in



Information from the USGS map of the same title.

Colorado is extremely remote, previous eruptions have inundated large parts of Colorado and surrounding states west to California, north to the Dakotas, south to Mexico, and east to the Mississippi River. Even moderate ashfall over such a wide area, combined with unfavorable weather conditions, could produce catastrophic-systemic impacts on the North American electric grid. Resulting climatic issues may substantially impact local, regional, and global energy demand, complicating long-term recovery.

Volcano in Colorado:

There is no recent history of volcanic activity in Colorado. However, the eruption of Mount St. Helens deposited trace amounts of volcanic ash onto the state of Colorado on May 18, 1980.

Human-Caused Hazards



Human-Caused Hazards (sometimes called *anthropogenic hazards*) refer to potentially destructive phenomena with their origins in human activity. Human-caused hazards are characterized by an element of human negligence, intent, or error, or the failure of a human-designed system, in the hazard's origins. Human-caused hazards may be highly complex, and may involve a series of unpredictable primary and secondary impacts.

Human-caused hazards which occur as a result of actions intended to produce substantial negative impacts to human life, property, or activities, are sub-categorized as *Deliberate*. Deliberate human-caused hazards include criminal activities like terrorism, sabotage, arson, cyber-attack, and other intentionally destructive activities with the potential to negatively impact human populations. Deliberate human-caused hazards constitute a particularly challenging sub-category of hazards due to their origins in intentional human activity. International and domestic trends in technology, trade, infrastructure development, transportation, communications, manufacturing, finance, and many other sectors, contribute to higher economic efficiency and many other benefits, but can also lead to increased interdependencies and vulnerabilities that hostile organizations like criminal syndicates and terrorist organizations, adversarial nation-states, or even highly motivated individuals may seek to exploit.

Because deliberate human-caused hazards are intended to exploit vulnerabilities and interdependencies, the organizations and individuals responsible for deliberate human-caused hazards typically attempt to leverage strategic asymmetric conflict dynamics to produce the greatest damage at the lowest cost to the perpetrator. These strategic asymmetric conflict dynamics often render deliberate human-caused hazards particularly difficult to forecast and mitigate.



Terrorism and organized crime tactics can bear superficial similarities. The image at top shows the aftermath of a vehicle bombing by Islamist militant organization Hezbollah. The image below illustrates the aftermath of an organized crime assassination in Israel. Methods may be similar, but rationale, targeting, and ultimate objectives can differ markedly between criminal and terrorist groups.

Crime versus Terrorism:

In contemporary international security terminology, both criminals and terrorists fall into a broader category of *Violent Non-State Actors*, or VNSAs. Both are included in the VNSA category because: 1) neither type of organization represents a state or government, and 2), both engage in violence, property destruction, or the threat of violence and property destruction in pursuit of their objectives. Likewise, both activities are unambiguously illegal, and therefore render any deliberate hazard to critical infrastructure a matter of criminal investigation and legal prosecution, with resulting implications for hazard management and response. However, while crime and terrorism often involve similar methods and techniques, they differ in their origins, motivations, and incentive structures. Organized crime is characterized as organized and often violent illegal activity intended to produce material benefits for a closed population, while terrorism is characterized as organized and violent illegal activity undertaken in pursuit of broader ideological goals, often in an attempt to influence or benefit a larger population.

The following list reflects four illustrative similarities and differences between criminal and terrorist behavior:

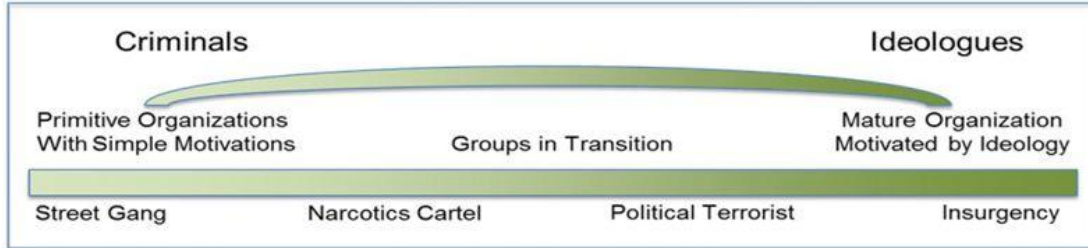
- **Both May Be Organized:** Both criminal and terrorist groups may be sophisticated and highly organized, or may be loosely networked, multi-cellular, organic, or individualist in structure.
- **Both Are Illegal:** Criminal and terrorist groups clearly engage in illegal activity, often involving premeditated violence.
- **Different Motivations:** While a terrorist group may seek financial benefit in the course of pursuing broader political, social, ideological, or theological goals, it is not primarily motivated by financial interests, and will generally seek to generate revenue only as a means to a greater end. In contrast, criminal organizations exclusively pursue financial interests over broader political or ideological goals. This demarcation between profit-seeking criminal groups and ideologically-motivated terrorist groups is sometimes referred to as the *transactional versus transcendent* divide.
- **Different Constituencies:** While terrorist groups or individuals often present their actions as intended to benefit a disaffected constituent population, or as intended to compel broader changes in social, political, or economic systems through force and the threat of force, organized criminal activities are intended to benefit only a closed group of constituents: those directly invested in the criminal organization and its activities. This delineation between organized political violence and criminal activities has many implications for prevention and response strategy.

Actor	Motivations	Strategic Approach	Target Selection	Operational Approach
Terrorist	<p><i>Political/Ideological</i></p> <p>Ideological objectives significantly influence organization's purpose and approach</p>	<p><i>Provocative/Attention-Seeking</i></p> <p>Pursues operations which produce maximum attention and political/social influence. May accept increased operational risk to achieve greater political impact</p>	<p>Maximize symbolic or destructive impact</p>	<ul style="list-style-type: none"> ✓ Symbolic targets ✓ Maximize public impact ✓ Aggressive clandestine Tactics ✓ Political demands
Criminal	<p><i>Financial</i></p> <p>Profit-maximization and evasion of law enforcement strongly influences organization's purpose and approach</p>	<p><i>Attention Avoidant/Risk-Adverse</i></p> <p>Seeks to minimize attention and risks to organization. Interested in business sustainability over achievement of ideological goals.</p>	<p>Maximize profits while minimizing risk</p>	<ul style="list-style-type: none"> ✓ Targets selected based on profit potential and risk profile ✓ Public impact unimportant or avoided ✓ Avoidant clandestine tactics ✓ Financial demands

The demarcation between "transactional" criminal actors exclusively interested in financial gain, and "transcendent" terrorist actors who see themselves as engaged in a grand ideological struggle, is not always clear.

Ideologically motivated organizations regularly engage in profit-generating criminal behavior in order to acquire resources for their larger ideological struggle, and some particularly powerful or competent criminal organizations have engaged in limited political or ideological violence as well. For example, the Taliban are an ideologically motivated Islamist/Nationalist organization which has engaged in terrorist attacks. The Taliban also derive a substantial portion of their financing through the illicit heroin trade. The fact that the Taliban's fundamentalist Islamist ideology eschews the trade and abuse of heroin, is ultimately insufficient to counteract the Taliban's practical interest in the tremendous profits the drug trade can provide, and the many ways in which this revenue can strengthen the organization and further serve its political and ideological interests. Likewise, powerful criminal organizations may engage in limited political violence intended to delegitimize law enforcement and state power, intimidate the public into compliance with its operations, prevent or discourage prosecutions, or to generally secure a favorable operating environment by demonstrating destructive capabilities and demanding concessions. Among criminal syndicates, such expansions into political violence often follow law enforcement crackdowns. Examples are numerous: various Italian mafia groups, Colombia's Medellin Cartel, and the numerous cartels involved in Mexico's ongoing Drug War, have engaged in political terrorism in response to government crackdowns, to list a small but representative sample.

The Violent Non-State Actor Continuum: From Transactional to Transcendent Violence



Graphic courtesy of: National Center for Security & Preparedness, SUNY-Albany

The motivational differences between criminal and terrorist actors has relevance to important elements of the attacker's strategic approach, these may include: target selection, willingness to negotiate terms, desire to evade law enforcement, need for public legitimacy, desire to acquire and retain financial benefits, and attention-seeking or desire for media coverage. Fortunately, many of the security processes and techniques intended to deter, prevent, and mitigate criminal behavior, can also deter, prevent, and mitigate terrorist behavior, and vice versa.

Criminal Exploitation of Critical Infrastructure:

Organized criminal threats against critical infrastructure and CI operators are comparatively rare. However, when they do occur, they typically reflect the profit-motivation of a criminal enterprise. Crimes of blackmail, theft, extortion, larceny, embezzlement, illicit trafficking, corporate espionage, sabotage, and data theft, may target critical infrastructure operators or exploit critical infrastructural vulnerabilities. The complexity of critical infrastructural systems and the dispersion of authority and oversight over these systems among a complex network of public and private sector operators and jurisdictions can produce security vulnerabilities potentially exploitable for profit by criminal actors.

Examples of this include criminal activities such as:

- The exploitation of complex supply chains, shipping, and tracking procedures to steal legitimate cargo in transit, or transport illicit cargo through apparently legal channels.
- The leveraging of knowledge about critical infrastructure operations or business, to sabotage critical facilities or systems for pay by a third party, or to threaten such sabotage as an extortion scheme.
- The theft of proprietary or sensitive data, or customer data, and the threat to disseminate such data as an extortion scheme or for payment by a third party.
- The penetration of a critical infrastructure operator's physical or IT security systems, and the threat of disruptions to operations or disclosure of information as an extortion scheme.
- The intentional destruction of key data or IT systems, or the threat of such destruction, as an extortion scheme or as a component of un-organized criminal behavior.

- Targeting of employees, staff, or executives for blackmail, extortion, or bribery, and potential enlistment of employees as accessories or directors of criminal activities.
- Systematic sabotage of wholesale and retail products as an extortion scheme.
- Large scale theft of critical data or assets for profit, unintentionally resulting in diminished ability to operate critical infrastructure, or respond to unrelated hazards.
- Each of the examples above can be differentiated from terrorist activity in that they are clearly and almost-exclusively profit motivated. The profit motivation of criminal organizations has significant impacts on choice of target, operational objectives, methods selected to evade investigators, and patterns of violent behavior, to name only a few potentially significant factors.



Critical infrastructure operators may be targeted for extortion. In 2004, a criminal organization planted explosives at multiple key locations in France's critical TGV rail network, demanding untraceable delivery of \$5 million or destruction of rail assets and potential loss of life. Security management attempted to comply with monetary demands while simultaneously applying strong investigative pressure, and screening large portions of the TGV network for explosive devices. While costly, these countermeasures eventually resulted in the extortion group withdrawing its demands without destruction of property or loss of life, and without receiving payment of the demanded ransom.

Implications for critical infrastructure protection are numerous. While sophisticated and well-resourced criminal enterprises often possess greater potential to disrupt critical infrastructure operations than terrorist groups, a criminal organization's motivation to sustainably generate profit while evading law enforcement is a disincentive to overly provocative or conspicuously violent behavior. Therefore, the strategic approach of a criminal group targeting critical infrastructure operators will typically be non-attention seeking, interested in operational security and evasion of law enforcement, and profit motivated.

These constraints on criminal behavior are a product of criminal incentive structure: a criminal actor wants to make money and escape to enjoy it, and is largely uninterested in pursuing any broader ideological objective. As a result, criminal organizations targeting critical infrastructure operators tend to gravitate toward

theft, extortionate crimes, and other exploitations of CI vulnerabilities through which revenue can be generated.

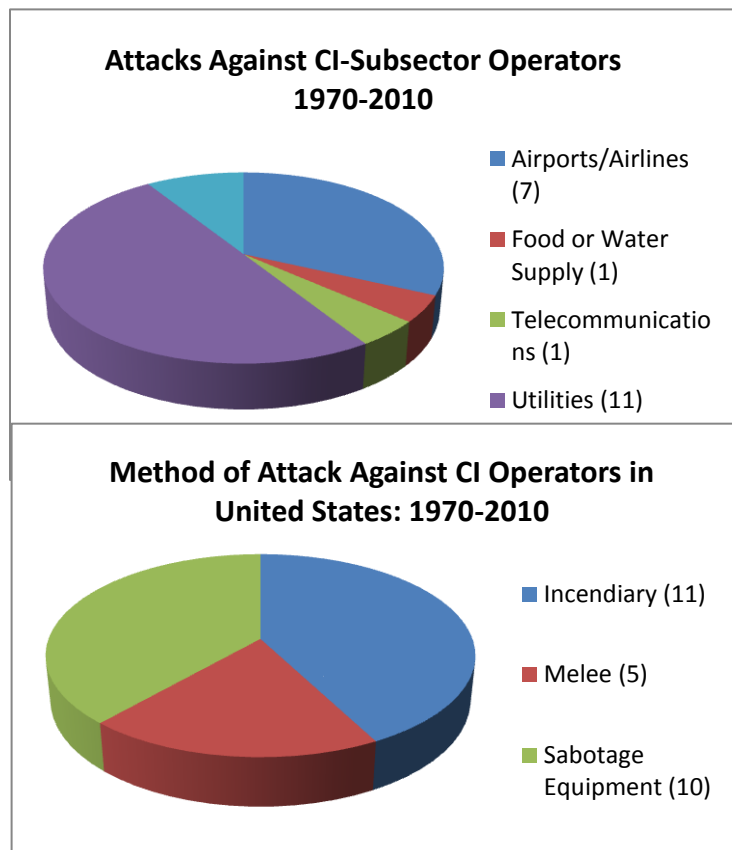
Implications for countermeasures are likewise numerous: Criminal organizations are profit and survival oriented, therefore countermeasures that increase the risks of apprehension, or the costs and challenges of successful evasion, often tend to be more effective against criminal threats than terrorist threats. Likewise, countermeasures that decrease criminal return on investment, either through increasing the costs of a criminal operation, or decreasing its potential benefits to

the criminal actor, will also dis-incentivize the targeting of critical infrastructure and critical business operations and assets. However, in contrast with terrorist organizations, which are typically interested in achieving some measure of public credibility or legitimacy, organized criminal enterprises are neither attention-seeking nor legitimacy-seeking. Countermeasures intended to decrease public support for a criminal organization, delegitimize a criminal organization in the eyes of the public, or to portray the organization as incompetent or non-credible, would therefore not be expected to significantly impact criminal behavior.

Unlike many terrorist activities, criminal activities exploiting critical infrastructural vulnerabilities are not intended to produce widespread psychological impacts. This may have implications for targeting and operational method: whereas a terrorist organization may select targets or operations in pursuit of maximum media attention, public impact, or communicative value, criminal organizations tend to prioritize revenue generation and evasion of law enforcement, and therefore tend to select targets with greater internal impact to the critical infrastructure operator or its dependent clients, and less interest in public impact or challenging of law enforcement.

Terrorist Exploitation of Critical Infrastructure:

Whereas criminal organizations are generally risk averse and almost exclusively interested in profit maximization, terrorist organizations ultimately intend for their operations to produce a larger political or social impact. The interest in producing maximum political and social impact is often carefully balanced against an occasionally contradictory interest in maximizing public credibility of the organization, and maximizing legitimacy of the organization's ideological causes. While terrorist objectives may at times appear irrational, the specific methodologies and tactics a terrorist organization utilizes are often the result of careful calculation.



Source: Global Terrorism Database, 2012

While organized crime groups typically restrain violent behavior to minimize risk, terrorist organizations may be willing to assume increased risk in order to maximize the destructive impact of their operations. This has

implications for terrorist objectives, strategy, tactics, and target selection, and usually differentiates terroristic threats from criminal threats. For example, a criminal organization may engage in corporate espionage in order to steal proprietary data for illicit sale, or to extort their target for payment, whereas a terrorist organization may engage in similar corporate espionage tactics to gain the information and access necessary to attack or sabotage critical infrastructure and cause maximum damage. Unlike most criminal threats, this terroristic threat may involve provocative attacks without warning or attempts at extortion.

Similarly, criminal hostage-taking for ransom, or threats against critical infrastructure for extortion payment, are usually undertaken in a serious attempt to secure payment. Under this transactional logic, provocative or escalatory criminal violence is dis-incentivized, as the criminal organization wishes to appear as a credible negotiating partner in order to secure payment and evade capture. In contrast, while terroristic hostage-taking and extortion plots have also followed a transactional logic at times, they may also reflect a transcendent logic which values the government and media attention that the attack will gain the organization. Under this transcendent logic, traditional constraints on violence against hostages or destruction of property without warning are potentially removed. Whereas a criminal hostage taker or extortionist may wish to conclude negotiations quickly in order to secure profit objectives, and has little use for media attention except to raise the pressure on law enforcement to prevent a violent outcome; a terrorist hostage taker may purposefully draw out negotiations or make unrealistic demands until media can arrive to publicize the violent outcome that the attackers had planned from the outset.

Like criminals, terrorists are aware of complex critical infrastructural interdependencies, and seek to exploit them. However, the provocative nature of terrorist strategy often translates into a higher prioritization of violent and destructive tactics. A few examples of terrorist threats to critical infrastructure follow:

- Physical attacks against CI operator assets, facilities, or personnel utilizing explosives, incendiaries, small arms, booby traps, or any number of manufactured or improvised conventional weapons.
- Sabotage of critical infrastructure, facilities, or systems intended to cause maximum disruption.
- Theft of CI operator data, or penetration of CI systems, in order to facilitate maximum impact of subsequent attacks.
- Attack on facilities which hold symbolic value for the terrorist organization, the target, or the public.
- Follow-on attacks targeting personnel and assets responding to a previous attack or threat.
- Physical attacks against CI operator assets, facilities, or personnel utilizing unconventional weapons or weapons of mass destruction (WMD), which may include toxins, poisons, radiological devices, chemical weapons, nuclear devices, biological agents, or any number of

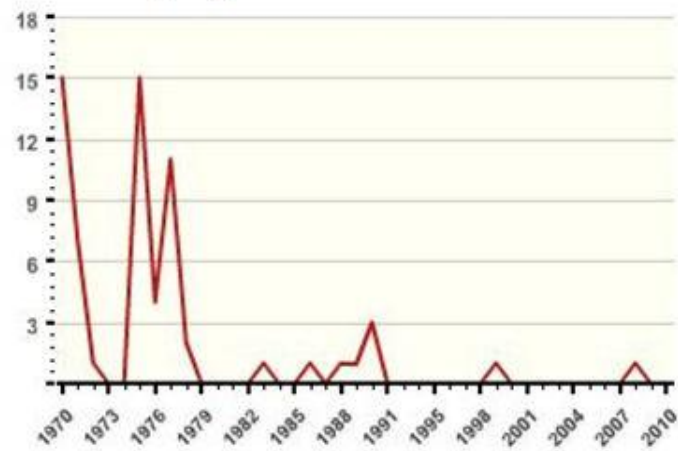
unconventional weapons or weapons designed to produce large scale destruction or casualties.

- Surveillance, dry runs, and penetration tests of CI operator infrastructure, systems, security, and procedures to maximize probability of successful attack.
- Targeting of executives, policymakers, staff, or other personnel with connections to CI operations.
- Cyber attacks intended to disrupt CI operations or damage CI components and assets.
- Targeting of assets based on potential for maximum disruptive impact or media attention.

In the United States, well-planned and coordinated attacks against critical infrastructure operators have been rare. The Global Terrorism Database lists a total of twenty one significant (non-cyber) terrorist operations targeting transportation, water supply, food supply, utility, and telecommunications infrastructure assets and facilities from 1970-2010. Though attacks on critical infrastructure within the United States are rare overall, *utilities and aviation operators are overrepresented as targets of terrorist attacks on critical infrastructure operators in the United States.*

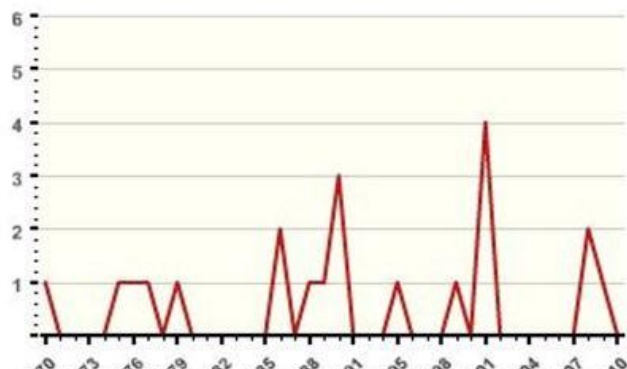
With this stated, attacks on utilities have generally declined since the peak of domestic terrorism activity against critical infrastructure during the 1970s. Though militant environmental groups in the United States do not appear to seek substantial human casualties, they are overrepresented in attacks involving destruction of utility and CI operator assets. Likewise, Islamist militant groups and individuals are overrepresented in attacks on US aviation assets, and right wing extremist groups and individuals are overrepresented in attacks on law enforcement and government facilities.

Attacks Targeting Utilities in United States: 1970-2010



Source: Global Terrorism Database, 2012

Attacks Targeting Transportation, Food/Water, Utilities, and Telecommunications Infrastructure in United States: 1970-2010



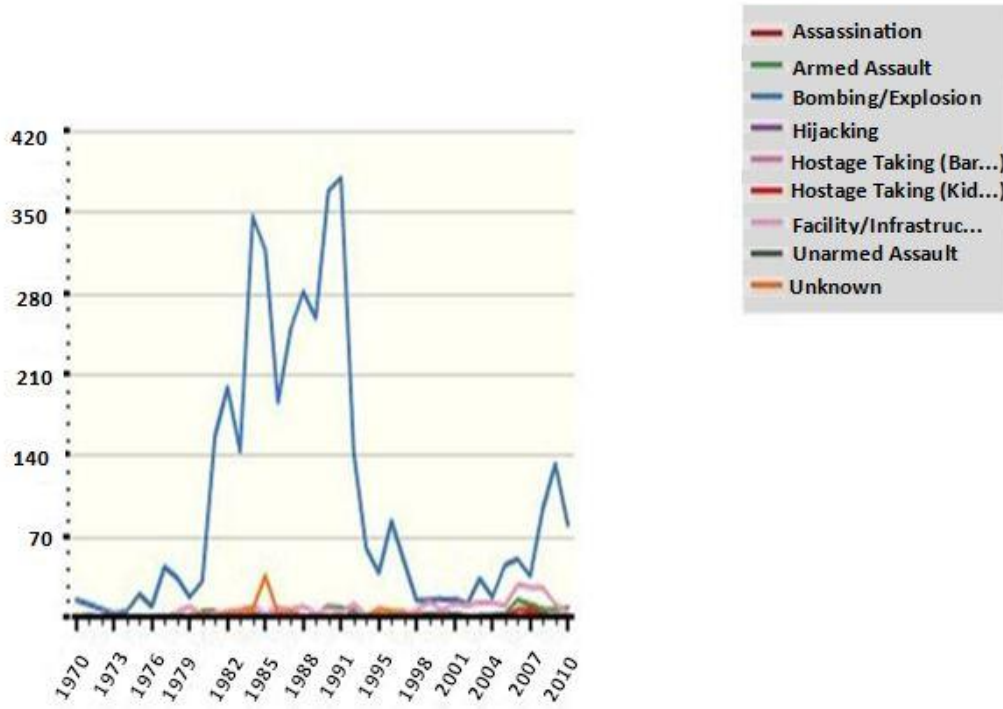
Source: Global Terrorism Database, 2012

These patterns are not suitable for reliable forecasting, but may inform CI operator security policies and countermeasures. For example, a credible threat originating from a militant environmental group would not typically be expected to result in target selection for mass casualties, and is more likely to involve sabotage of vulnerable equipment and components, particularly via arson or incendiary device. Likewise, a credible threat originating with a fundamentalist religious terrorist group like al-Qaeda, is more likely to involve target selection for maximum casualties and public impact, sometimes through spectacular methods intended to produce maximum media attention. Accordingly, al-Qaeda has targeted aviation assets for attack. These assets are critical infrastructural, high profile, and contain the potential for high casualties.

Because environmental groups have been overrepresented in attacks on utilities in the United States, methods traditionally embraced by these groups such as sabotage and arson have been overrepresented as well. The overrepresentation of melee weapons in attacks against critical infrastructure is exclusively indicative of al-Qaeda's unusual and tactically effective reliance on melee weapons in the coordinated attacks of September 11, 2001, and may not reflect a general trend. Equipment sabotage may be accomplished through a variety of methods. The majority of sabotage attacks in the United States have involved tampering or arson rather than explosives.

While only twenty six major incidents of terrorist attack against critical infrastructure operators have been recorded in the Global Terrorism Database, the data implies a much stronger historical basis for critical infrastructural attacks outside the United States. Between 1970 and 2010, there were 4457 incidents against critical infrastructure operators worldwide. Explosive attacks intended to kill personnel or destroy property are overrepresented as the method of choice for attacks against critical infrastructure operators outside the United States. Note that this survey of attacks against critical infrastructure operators is limited to physical, rather than cyber attack. Information specific to cyber threats is provided in the eponymous reference section.

Attacks Worldwide Targeting Utility, Transportation, and Telecommunications Sectors by Attack Type: 1970-2010



Source: Global Terrorism Database, 2012

Terrorist attacks typically follow a loosely defined cycle of preparation, implementation, and escape. The full attack cycle is defined below:

- 1) **Initial Planning & Target List Development:** The terrorist organization will begin general logistical planning and develop a list of potential targets.
- 2) **Initial Surveillance & Target Selection:** The organization will begin surveillance and evaluation of a selection of potential targets. Once a target or targets have been selected, logistical and operational planning becomes increasingly customized for the targets selected.
- 3) **Surveillance:** Organization may escalate surveillance of selected targets in preparation for attack. More advanced techniques may include technical surveillance measures or penetration testing of the target or a location/asset with similar characteristics to the target.
- 4) **Rehearsal:** Organization engages in dry runs and final rehearsals.
- 5) **Attack:** The terrorist operation is carried out.
- 6) **Escape & Exploitation:** Terrorists and/or handlers and managers attempt to escape apprehension, and exploit any gains in information or position resulting from the attack. This stage is applicable even in most cases of suicide attack in which handlers, trainers, logistical personnel, or managers must evade apprehension to engage in future attacks.

Terrorist Attack Cycle



Each of these stages exposes terrorist personnel to increasing levels of risk. Effective intervention and prevention is possible at any stage of the attack cycle, but becomes substantially more difficult at stages five and six.

Each stage of the attack cycle involves different indicators that can potentially expose the plot to law enforcement or intended victims, and some profiling indicators may provide law enforcement and critical infrastructure operators an approximation of how far the terrorist organization has proceeded on the attack cycle timeline. It is worth noting that many of the early phase indicators are not necessarily illegal behaviors, and may have a legitimate explanation. When indicators are ambiguous, further monitoring of potential suspects is often recommended until a more accurate determination can be made.

Examples of Potential Profiling Indicators and Counterstrategies by Attack Phase		
Attack Phase	Potential Indicators	Potential LE/CI Operator Response
Stage 1: Planning & Target List	<ul style="list-style-type: none"> ▪ Theft or unauthorized access to CI data, particularly data involving vulnerabilities ▪ Data mining ▪ Penetration of CI systems ▪ Consultation of obscure documents and sources on CI ▪ Dispersal of information gathering efforts to avoid scrutiny 	<ul style="list-style-type: none"> ▪ Law enforcement/CI stakeholder surveillance, reporting, and monitoring
Stage 2: Initial Surveillance Target Selection	<ul style="list-style-type: none"> ▪ Suspicious trespassing/surveillance of potential CI targets ▪ Systematic trespassing/surveillance of multiple potential CI targets ▪ Active counter-surveillance efforts ▪ Human engineering, hacking, or other clandestine efforts to gain physical or virtual access to CI facilities or systems ▪ Systematic surveillance of specific CI sub-sectors or specific types of assets and facilities ▪ Construction or acquisition of weapon components or precursor materials. 	<ul style="list-style-type: none"> ▪ Increased surveillance, reporting, and CI operator information sharing ▪ CI operator security/counter-surveillance measures ▪ CI Operator security/threat assessment ▪ Increased CI operator vigilance
Stage 3: Surveillance	<ul style="list-style-type: none"> ▪ Systematic clandestine surveillance of specific target assets or facilities ▪ Acquisition of uniforms, credentials, vehicles, or other logistical resources to facilitate physical penetration or access to target ▪ Physical or virtual penetration testing ▪ Construction or acquisition of specific weapons or tools necessary to carry out attack ▪ Planning and preparations for attack and exploitation phases ▪ Time trials ▪ Diversionary tactics to surveil response capabilities 	<ul style="list-style-type: none"> ▪ Intensified surveillance, reporting, and Law Enforcement/Stakeholder information sharing and coordination ▪ CI Operator security increase ▪ Increased CI operator counter-surveillance ▪ Preparation for intervention ▪ Intervention
Stage 4: Rehearsal	<ul style="list-style-type: none"> ▪ Surveillance abruptly decreases or terminates ▪ Prepositioning of resources ▪ Increase in clandestinity ▪ Diversionary tactics to increase law enforcement interest in other plots or targets 	<ul style="list-style-type: none"> ▪ Intensified CI operator vigilance and security increase ▪ Continual Law Enforcement/Stakeholder information sharing ▪ CI Operator threat-customized mitigation ▪ Preparation for intervention ▪ Intervention
Stage 5: Attack	<ul style="list-style-type: none"> ▪ Indicators are situation-dependent 	<ul style="list-style-type: none"> ▪ Law Enforcement, Stakeholder, or CI Operator protective operations, response, and recovery
Stage 6: Escape & Exploitation	<ul style="list-style-type: none"> ▪ Destruction/disposal of evidence ▪ Planting of evidence intended to mislead investigators ▪ Physical escape along pre-coordinated routes ▪ Ties cut between surveillance/logistics/operations cells ▪ Assumption of new identity/cover/legend ▪ Sacrifice of personnel least likely to survive, or most likely to escape conviction ▪ Public information/credit seeking/false or misleading credit seeking 	<ul style="list-style-type: none"> ▪ Evidence + records preservation ▪ Stakeholder/CI Operator investigative support to law enforcement ▪ Stakeholder damage assessment, after action reporting, lessons learned, and preventive/mitigative efforts against future attack

In analyzing deliberate threats to critical infrastructure, it is also necessary to differentiate between methods disruption of critical infrastructure as a primary objective, and methods that kill CI operator personnel or cause destruction of operator assets as a secondary objective. While major attacks against non-CI operators can impact or disrupt critical infrastructural operations, the most practical methods for attack against critical infrastructure may differ from the methods selected against civilians and non-CI business and government assets. Some of these differences in method and target selection are described in more detail in the individual hazard reference sections.

Nuclear Attack

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
State-Regional	Catastrophic	None (by NSA)	Extremely Rare	Catastrophic	58.26

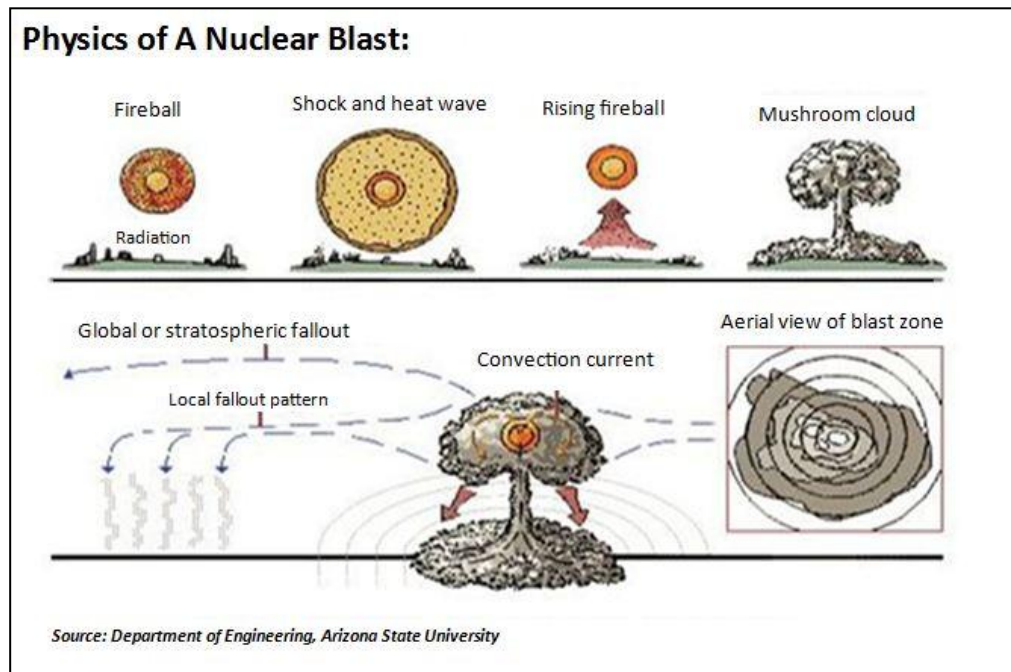
General Summary: Nuclear attack refers to the intentional detonation of a device deriving its destructive force from nuclear reactions. Nuclear weapons may be fission or fusion based, the technical differences in design are relevant primarily in terms of yield and the technical difficulties of manufacture; with fusion or thermonuclear devices requiring considerable technical capability to manufacture, and yielding greater destructive force by payload size. In military

applications, nuclear warheads may be delivered by a variety of means including ballistic missile, cruise missile, gravity munitions, artillery shell, mine, surface to surface missile, and man-portable tactical case.

Military-grade nuclear weapons

are referred to as tactical or strategic. Tactical warheads are designed for battlefield applications, and tend to be lower-yield, lighter weight, more portable, and deliverable by shorter-range methods such as artillery shell, vehicle delivery, mine, or hand-transport.

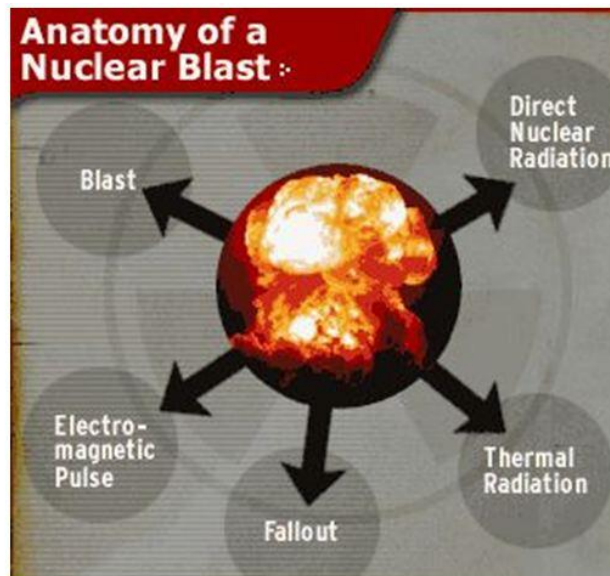
Strategic weapons are comparatively high-yield, and are designed to produce the heavy and wide-scale destruction necessary to virtually halt government operations and productive activity within major metropolitan areas or strategic centers. Strategic weapons differ from tactical weapons in yield, size, weight, portability, component materials, and delivery systems, and generally require nation-state resources to manufacture and deploy.



Because the manufacture of even a basic "gun barrel" type of tactical fission device requires sophisticated logistical, supply chain, manufacturing, and technical capabilities, the open or clandestine full-cycle manufacture of a deployable nuclear weapon has been accomplished by only a handful of governments, and would be a serious challenge to any non-state actor. As the prospect of unprovoked nuclear attack against the United States by a nuclear power utilizing strategic nuclear devices is currently considered remote, and the full-cycle manufacture of a nuclear weapon would be difficult for a non-state actor, this entry will concentrate on the potential for a tactical nuclear device to be manufactured by a terrorist group from weapon-ready materials obtained on the illicit market, or delivered to a terrorist group by a hostile government.

In the case of terrorist attack utilizing an improvised or military grade tactical nuclear weapon, mode of delivery would likely be via physical transport of the weapon to an urban center via road, rail, or aviation assets, or assembly of the weapon at its point of detonation in an urban center, rather than through a military delivery system such as a cruise or ballistic missile. The demands of clandestine manufacture virtually guarantee that a warhead produced by a non-state actor would go untested until deployment.

Potential Impacts: Nuclear detonations produce powerful blast and heat, and varying outputs of radiation, radioactive fallout, and electro-magnetic pulse and should be considered as a High Impact/Low probability event. These impacts are dependent on weapon design, mode of delivery, and environmental factors near detonation. Warheads theoretically deployable by a non-state terrorist organization could range from relatively low-output man-portable tactical devices ranging between 1-20 kilotons, to smaller strategic devices decoupled from their military-grade delivery systems, potentially ranging between 100 kilotons-3 megatons. Some debate persists regarding the likelihood of a terrorist organization acquiring a deployable nuclear device, and whether terrorist organizations would be willing to detonate a nuclear device if they did successfully acquire one, rather than use their possession of a nuclear device for leverage in negotiating concessions. Most terrorist organizations are unlikely to acquire a nuclear device, and may be unlikely to detonate a nuclear device even upon acquisition. However, a terrorist organization willing and able to deploy a nuclear device is likely to select targets for maximum casualties, public impact, and/or symbolic impact.

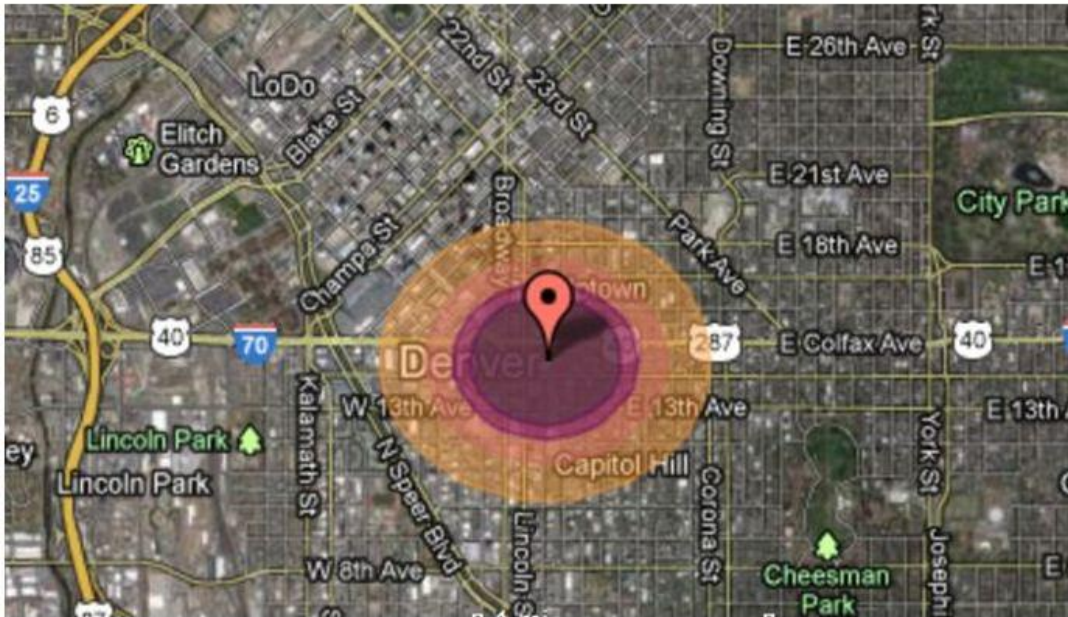


Source: United States Congress' Office of Technology Assessment report: "The Effects of Nuclear War"

Detonation of a nuclear weapon by a terrorist organization is more likely to occur in a high-profile urban area with significant economic, social, and government activity, rather than a lower-density suburban or rural area where more significant infrastructure disruption can be sought in exchange for a lower overall area denial, property damage, casualty rate, and impacts to government and business operations.

Potential Energy Sector Impacts: *Catastrophic.* While destructive impacts of nuclear devices are highly variable depending on type of device and the method and location of delivery, virtually all above-ground energy infrastructure, facilities, and offices within blast and thermal damage ranges would be destroyed or severely damaged. Unprotected personnel sufficiently within blast, thermal, and ionizing radiation thresholds would experience high casualty rates. Moderate to high-yield military-grade devices delivered via airburst would potentially release a pulse of electromagnetic radiation the effects of which on energy and telecommunications infrastructure would be similar to a rapid-onset and extremely severe geomagnetic storm event. Ground burst delivery is more likely to be utilized by a terrorist organization, and may produce similar electromagnetic impacts on infrastructure, but on a much smaller geographic scale. Irradiation of areas within and surrounding the blast zone would produce area-denial impacts, producing casualties and increasing the risk and difficulty of accessing and servicing impacted areas. Underground assets such as pipeline and communications nodes would be damaged or destroyed depending on blast proximity and total overpressures. The targeting of a major urban center may result in severe or catastrophic impacts to local or regional energy sector and government operations depending on location of primary and secondary coordination and control facilities relative to blast, thermal, and radiation zones.

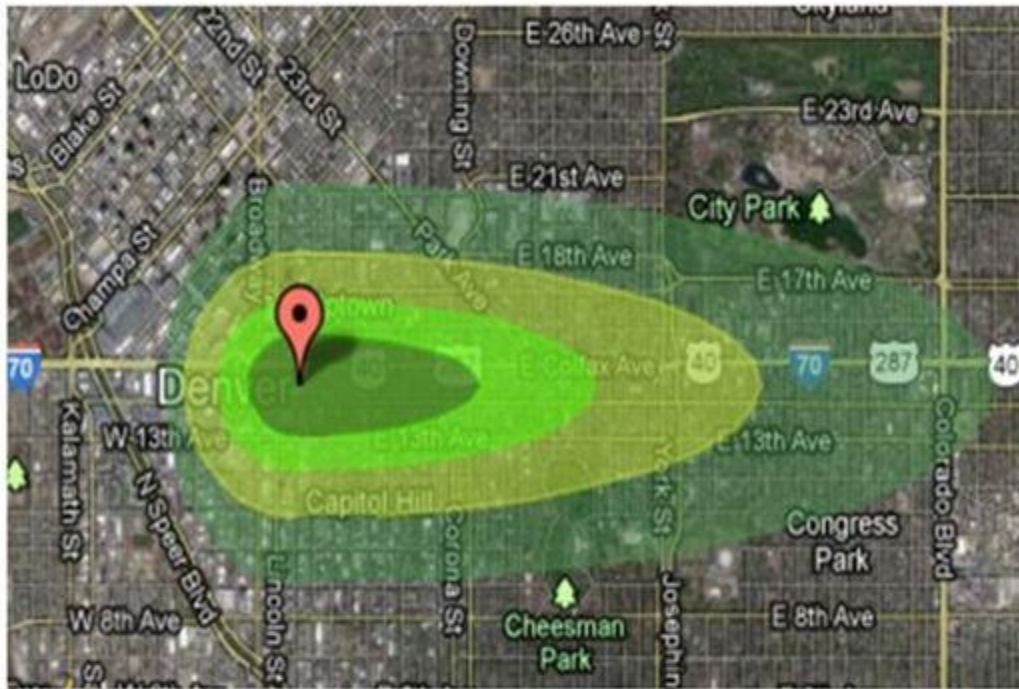
1 Kiloton Ground Detonation of Tactical Nuclear Weapon at Colorado State Capitol: Thermal Effects



Zone	Physical Effects
First degree burns	Sunburn-like discomfort, skin redness
Second degree burns	Blisters and pain, like burns by boiling water
Third degree burns	Skin charring and necrosis, requiring medical care
Conflagration	Most people will die within 24 hours

Source: CarlosLabs Ground Zero II Nuclear Impact Modeling Software

1 Kiloton Ground Detonation of Tactical Nuclear Weapon at Colorado State Capitol: Fallout Modeling (Assuming Winds Due East 8-12 mph)



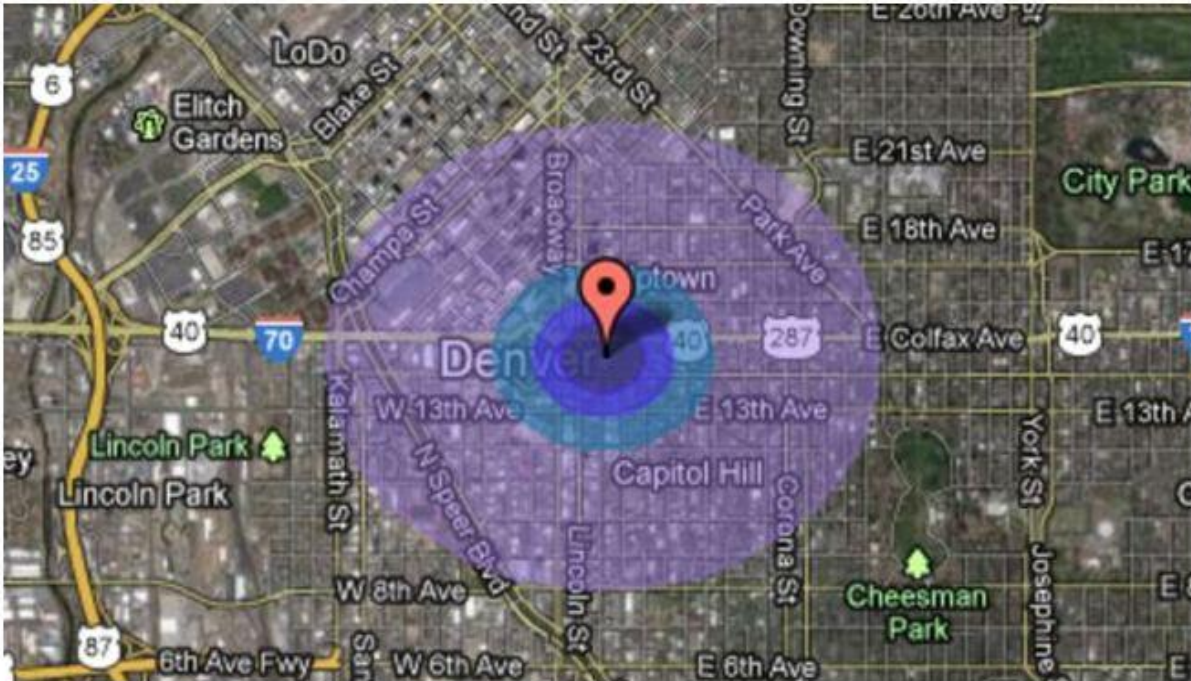
Zone	Physical Effects
< 200 REM	Nausea with long-term risk of cancer
200 - 500 REM	Bleeding, vomiting, hair loss, 10-30% fatalities
500 - 800 REM	Bone marrow destruction, coma, 50-70% fatalities
> 800 REM	Fatalities approach 100% within 24 hours

Source: CarlosLabs Ground Zero II Nuclear Impact Modeling Software

Thresholds for Severe Damage or Total Loss by Explosive or Nuclear Overpressure:	
Light Construction/Residential Construction	5 psi
Brick Structures/Commercial Construction	10 psi
Reinforced Concrete Structures	20 psi
Nuclear Weapon Storage Bunkers	100-500 psi
Command Bunkers	100-1000 psi
Missile Silos	500-10,000 psi
Deep Subterranean Command Bunkers	1000-100,000 psi

Source: Globalsecurity.org

1 Kiloton Ground Detonation of Tactical Nuclear Weapon at Colorado State Capitol: Blast Effects



Zone	Physical Effects
1 psi (6.9 kPa)	Windows shatter, injuries by shards and debris
5 psi (34.5 kPa)	Non-reinforced structures fail and collapse
10 psi (69 kPa)	Quake-proof buildings are totally destroyed
20 psi (138 kPa)	Fortifications and bunkers are demolished

Source: CarlosLabs Ground Zero II Nuclear Impact Modeling Software

Radiological Attack

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
Localized	Moderate	None(via RDD)	Rare	Slight	31.49

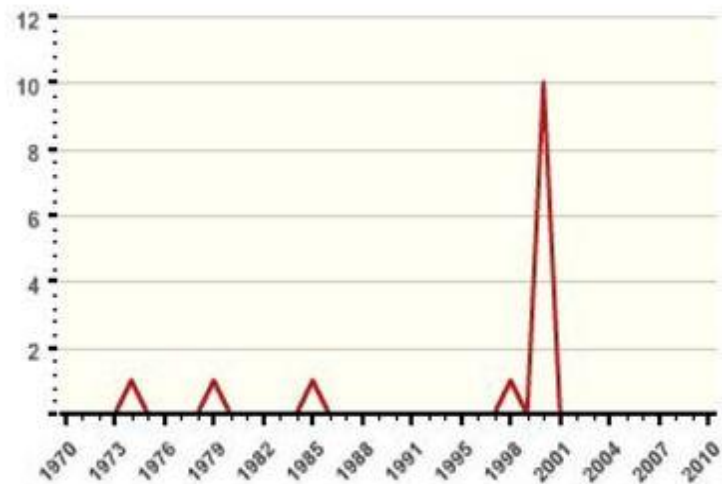
General Summary: Radiological Attack refers to the use of radioactive materials to injure or kill personnel, or to produce area-denial effects via radioactive contamination. Radioactive attacks may include physical delivery of contaminants to discrete target areas, or by use of radiological dispersal devices to spread radioactivity over a wider area. Radiological dispersal devices, commonly referred to as "dirty bombs" or "salted bombs," are weapons intended to disperse radioactivity via conventional explosive and nuclear warhead detonation, respectively. Salted bombs are military-grade nuclear warheads customized to produce large quantities of radioactive fallout. There are no open source records indicating that Salted Bombs are currently maintained by any government, and both conventional and nuclear radiological dispersal devices are today considered impractical and undesirable as military weapons. In addition, the technological and nuclear supply chain prerequisites for the construction of a salted bomb render the potential of acquisition and use of a salted bomb by criminal or terrorist groups extremely remote.

Therefore, in this hazard entry, the term "radiological dispersal device" will apply to "dirty bombs" which utilize conventional explosives to disperse radioactivity. Radioactive materials may also be physically delivered as a powder or metal, or atmospherically dispersed as a gas or aerosol.

Physical delivery of radioactive materials without explosive dispersion exclusively constitutes the historical record of radiological terrorist attack. Although some terrorist actors have allegedly plotted

to fabricate and employ radiological dispersion devices, open source records do not indicate that terrorist efforts to construct and use a dirty bomb have ever succeeded. The fortunate lack of historical cases of RDD use, render modeling and estimates of RDD construction, deployment, and impacts, to be somewhat speculative.

Radiological Attacks Worldwide: 1970-2010



Source: Global Terrorism Database, 2012

Likewise, due to the low dispersion, relatively low contamination levels, and lack of area-denial effect of non-explosive radiological attacks for which there are historical cases, radiological attacks worldwide without a dispersal device have primarily been limited to disorganized lone wolf attacks against symbolic offices and individuals, and sophisticated assassination attempts.

Potential Impacts: A well-constructed RDD, deployed effectively under favorable conditions, could produce significant disruptive and area denial effects. Estimates of levels and extent of radiological contamination vary widely depending on device type, construction, and on a variety of environmental factors that can be difficult to model. Recent studies indicate that effective emergency management and public health management in the wake of an RDD attack could minimize long-term hazards to human health, limiting most of the impacts of RDD use to the damage caused by the conventional explosive detonation, economic damage to contaminated areas, and the socio-psychological and emergency management costs of cordoning and decontaminating exposed areas and their residents, and managing subsequent traffic into affected areas to prevent unacceptable exposure. Though precursor materials for the manufacture of an RDD are potentially available through licit and illicit channels, the challenges of clandestinely acquiring precursors as well as the technical knowledge and fabrication tools while evading law enforcement, are significant. Transport of a higher-lethality RDD over significant distances to deliver it would require heavy shielding materials to avoid detection. This shielding would have to be removed prior to detonation, exposing the device to detection and its deliverers to significant radiation.

Potential Energy Sector Impacts: *Slight.* Radiological attack is not an attractive method by which to disrupt critical infrastructure operations. The greatest costs incurred by radiological dispersal devices are a product of the economic and psychological results of contaminating an area of dense population and economic activity. The radiological impacts of the devices themselves are not any more damaging to critical infrastructure than the conventional explosive payload utilized for the dispersal, serving only to complicate recovery efforts if critical infrastructure were to be damaged in the explosive detonation. Further, a terrorist organization considering the prospects of critical infrastructural attack would be likely to conclude that the risks and drawbacks of utilizing a radiological weapon exceed any likely disruption to infrastructure, and that more effective methods of attacking critical infrastructure can be pursued with lower risk and resource investment. However, a highly successful attack utilizing an RDD within a dense urban environment would likely produce contamination requiring quarantine or extraordinary precaution when accessing critical components, therefore increasing costs and decreasing access to infrastructural components by CI operators.

Explosive Attack

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
Localized	Severe	Periodic	Moderately Likely	Severe	55.41

General Summary: Explosive hazard refers to the use of conventional explosive materials to damage or destroy grid components, assets, or facilities, or to injure and kill energy sector personnel with the objective of disrupting energy sector operations. Pyrotechnic and incendiary devices are sometimes characterized as explosive devices, though they work through different physical principles than conventional explosives, and are included in the "Physical Attack" category of this reference guide. Conventional explosives are chemical or pressurized gas compounds which contain high potential for energy release. When high explosive charges are detonated, they produce light, heat, sound, and pressure expansion faster than the speed of sound. Explosive fragmentation devices are designed to disperse shrapnel ahead of the blast wave to increase anti-materiel and anti-personnel effects, while non-fragmentation devices such as thermobaric weapons cause damage primarily through overpressure.

There are a wide variety of explosive compounds, some of which are highly sensitive, and can be detonated directly through the introduction of relatively small amounts of heat or pressure, and some of which are insensitive and highly stable, and must be detonated through the primary detonation of another explosive. Relatively sensitive and unstable explosives which can be detonated directly are referred to as primary explosives, and relatively insensitive and stable explosives which must be detonated by other explosives are referred to as secondary explosives.

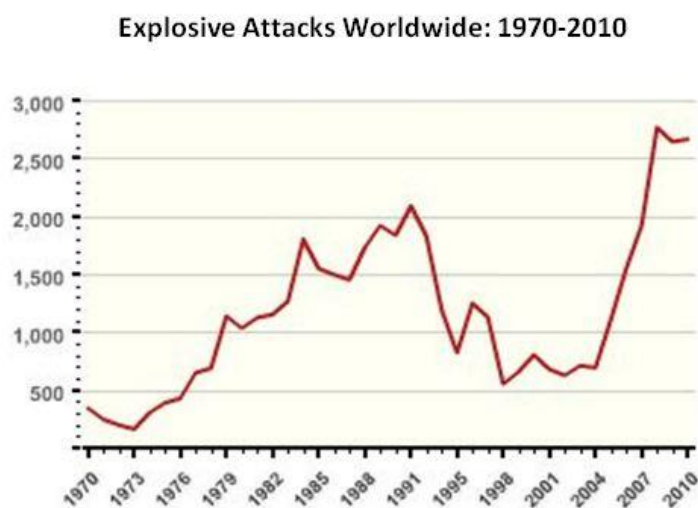
Materials Commonly Used in Improvised Explosive Devices

	Common uses	Common form	Known IED use
High explosives			
Ammonium nitrate and fuel oil (ANFO)	Mining and blasting ²	Solid	Oklahoma City bombing
Triacetone Triperoxide (TATP)	No common uses; mixed from other materials	Crystalline solid	2005 bombings in London
Semtex, C-4	Primarily military	Plastic solid	Irish Republican Army bombings
Ethylene glycol dinitrate (EGDN)	Component of low-freezing dynamite	Liquid	Millennium Bomber, intended for Los Angeles airport, 1999
Urea nitrate	Fertilizer	Crystalline solid	World Trade Center 1993
Low explosive			
Smokeless powder	Ammunition	Solid	Olympic Park bombings

Source: IED ATTACK: Improvised Explosive Devices Fact Sheet. http://www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet.pdf

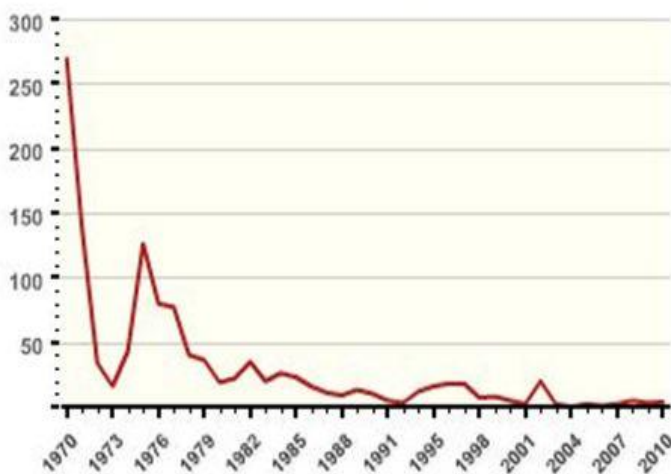
Both types of explosives are capable of producing significant damage and injury with sufficient quantity and placement. Many industrially-manufactured explosive compounds are permeated with chemical markers which render them detectable to explosive-sniffing dogs and explosive screening devices, likewise some screening devices are configured to detect a selection of improvised compounds. However, some industrially-manufactured explosives and improvised

explosive compounds are difficult to detect through rapid screening methods. Sophisticated criminal enterprises or militant organizations may divert from legal markets or otherwise acquire reliable and ready-to-use industrially manufactured explosives which require little customization or packaging before delivery, but less sophisticated organizations and individuals often attempt to manufacture improvised explosive devices from precursor chemicals and otherwise legal materials, leading to longer preparation timelines.



Source: Global Terrorism Database, 2012

Explosive Attacks in United States: 1970-2010



Source: Global Terrorism Database, 2012

produce more powerful and directed blast waves capable of damaging or destroying armored vehicles and hardened structures. Vehicle-borne devices can carry larger quantities of explosive material, and generally do more damage.

Precursor compounds are necessary for explosive manufacture, but some of these precursor compounds are dual-use and cannot be fully controlled. Monitoring of logistical and preparatory attack phases and disruption of operational planning by law enforcement can be a legitimate and effective preventive action. Crime Prevention Through Environmental Design (CPTED) and facilities security techniques, involve personnel training, planning, screening, and procedures, standoff distance, and facility hardening against explosive threats, and can be effective risk reduction and mitigation strategies.

Explosives can be introduced in a variety of forms for which countermeasures are costly. Impacts depend on payload size, construction, placement, and composition. Blast and shrapnel effects typically radiate equally in all directions from detonation, but are attenuated by the size and density of obstructions. Shaped charges or explosively formed penetrators utilize this principle to

The use of explosives by criminal or political organizations typically reflects a multiphase process involving logistical coordination, device acquisition or manufacture, target selection, target surveillance, packaging, and delivery. As with other types of terrorist plots, an attack utilizing explosives may be most effectively disrupted before the packaging and delivery phases, after which point disruption of the terrorist operation becomes more difficult. Explosive devices may be delivered by a variety of transport methods. Attacks involving explosives often reflect sophisticated coordination and planning capabilities, and targets and payloads may be selected to leverage infrastructural vulnerabilities, maximize casualties or property destruction, or produce secondary impacts such as detonation of nearby fuels, conversion of nearby materials to shrapnel, blast wave focusing, or follow-on attacks targeting first responders.

Explosive attacks are relatively infrequent within the United States, and have been in general decline since the peak of explosive use by domestic terrorist organizations in the 1970s. Electrical infrastructure has been targeted effectively for explosive attack by terrorist and insurgent organizations abroad, but direct attacks utilizing explosives against utilities in the United States have been rare. Nevertheless, explosive attacks have been a consistent option for domestic and international terrorists targeting the United States in the past, and the potential for explosive use against critical infrastructural assets within the United States remains significant and is unlikely to rapidly decline.

Explosive Payload Size and Minimum Evacuation/Standoff Distances

Threat	Threat Description	Explosive Capacity	Building Evac. Distance	Outdoor Evac. Distance
	Small Package/Letter	1 lb	40 ft	900 ft
	Pipe Bomb	5 lb	70 ft	1,200 ft
	FedEx Package	10 lb	90 ft	1,080 ft
	Vest/Container Bomb	20 lb	100 ft	1,700 ft
	Parcel Package	50 lb	150 ft	1,820 ft
	Compact Car	500 lb	320 ft	1,900 ft
	Full Size Car /Minivan	1,000 lb	400 ft	2,400 ft
	Van/SUV/Truck	4,000 lb	640 ft	3,800 ft
	Delivery Truck	10,000 lb	860 ft	5,100 ft

Source: U.S. Technical Support Working Group (TSWG), Department of Homeland Security and National Academy of Sciences, *IED ATTACK: Improvised Explosive Devices Fact Sheet*.
http://www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet/pdf

Potential Impacts: Explosive devices may have widely varying impacts depending on size, composition, construction, placement, and application. A large vehicle-borne payload could potentially damage or destroy critical assets as large as industrial facilities, office buildings, or small office complexes. Explosives are sometimes utilized by more sophisticated terrorist organizations as components of coordinated multi-target attacks. Depending on the criminal or militant organization's target selection process, targets may be selected to maximize casualties, property destruction, impact to infrastructure and services, or media attention.

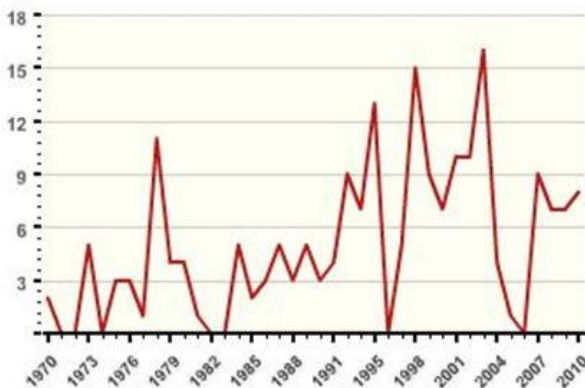
Potential Energy Sector Impacts: *Severe.* All explosives are a serious hazard to personnel located within minimum standoff distances, regardless of payload size. Small payloads may be sufficient to critically damage assets such as substations, transformers, or transmission towers. Mid-range to large vehicle-borne explosive payloads pose a serious hazard to large facilities. However, vulnerabilities differ substantially depending on facility construction and standoff distances, and must be evaluated via case by case facility security surveys. Nevertheless, substantial systemic disruptions could be produced by a coordinated explosive attack against key components at multiple grid locations. Such an attack would reflect unusual sophistication and aggressiveness for a domestically-based terror attack against US critical infrastructure operators, but remains a potentially severe hazard if employed by competent and coordinated adversaries.

Chemical Attack

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
Localized	Catastrophic	Rare	Rare	Slight	34.99

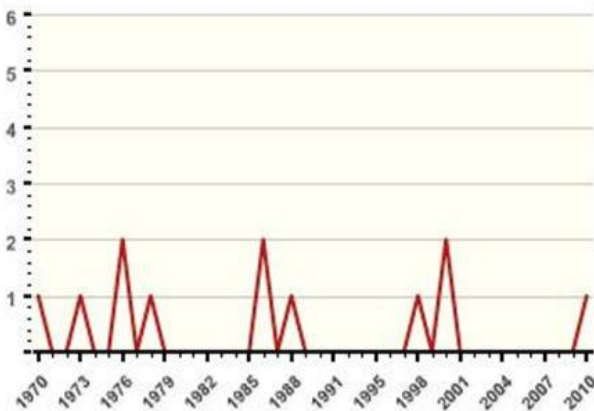
General Summary: Chemical attack refers to the application of toxic chemical substances as weapons. Chemical weapons may be utilized to achieve objectives ranging from injuring, killing, or incapacitating personnel to providing for area denial and compulsory decontamination. Chemical weapons are classified by their method of impacting the human body, and by their *persistence*, or, the length of time that the agent remains effective in an environment. While

Chemical Attacks Worldwide: 1970-2010



Source: Global Terrorism Database, 2012

Chemical Attacks in United States: 1970-2010



Source: Global Terrorism Database, 2012

nation-states are most capable of utilizing chemical weapons effectively, the threat of nation-state chemical attack against the domestic United States is considered extremely low. This entry will therefore concentrate on the potential for a non-state actor to utilize chemical agents in a terroristic attack within the United States.

Nation-states maintain stockpiles of military-grade chemical agents and effective dispersal systems. Some terrorist organizations have manufactured, or have sought to manufacture, military-grade chemical agents, but the challenges to clandestine manufacture and effective deployment are significant. Manufacture or acquisition of toxic industrial chemicals by a non-state actor utilizing dual-use technologies is a more probable scenario than the successful clandestine full-cycle manufacture of significant stockpiles by a non-state actor.

Likewise, a competent terrorist group seeking to cause significant casualties via chemical warfare, would find a direct physical attack and sabotage of urban industrial chemical facilities less challenging

than the full-cycle manufacture and deployment of chemical weapons, and such an attack may in fact have far greater casualty potential.

In all cases, the effectiveness of chemical attack is highly dependent on agent used, type of dispersal system, density of target area, and prevailing weather. Some analysts believe that chemical weapons would be unattractive for most terrorist organizations due to the challenge of manufacture or acquisition and risks of discovery, combined with the difficulty of effective deployment and potential for public or law enforcement backlash. Many political terrorist organizations are likely to reject chemical weapons in preference for conventional weapons which are easier to acquire and employ, and often produce equivalent or greater impact, whereas some apocalyptic religious organizations have displayed an unusual preoccupation with chemical weapons and other high profile weapons of mass destruction, combined with a lack of restraint brought on by abstract religious objectives, rather than concrete political goals. Analysts observe that the diffusion of dual-use industrial chemical production technology, and the continued prevalence of religious extremist groups, makes realistic the possibility of major chemical attack by a non-state actor.

Potential Impacts: By method of attacking the human body, chemical weapons are typically categorized as *nerve*, *asphyxiant/blood*, *vesicant/blister*, and *choking/pulmonary*. Higher persistency agents may remain effective in low concentrations, or may be treated with thickeners to enable it to coat surfaces for additional area denial effects. Most lethal chemical agents must be dispersed as a powder, aerosol, vapor, or liquid for effective introduction through inhalation or contact. Delivery methods intended to produce inhalation hazards tend to produce the most wide-ranging impacts, and tend to produce more rapid absorption of lethal dosages, as well as more rapid onset of symptoms.

Countermeasures, prophylaxis, and treatment are viable for most chemical weapons, but rapidity of detection, minimization of exposure, prophylaxis, and treatment are crucial to survival outcomes. The psychological impact of chemical attack on a civilian population can be disproportionate to actual lethality. Likewise, the financial and



Rarely, terrorist organizations have been capable of acquiring or manufacturing chemical weapons. The apocalyptic Japanese cult Aum Shinrikyo engaged in two attacks utilizing the nerve agent Sarin during the 1990s, resulting in 21 deaths, thousands of hospitalizations, and millions in decontamination costs. Other terrorist organizations are known to have sought chemical weapons for potential use.

Fortunately, it is difficult to clandestinely transport and effectively deliver most chemical weapons, and without sophisticated dispersal systems even military-grade chemical weapons are unattractive for area-denial attacks against infrastructure. Aum Shinrikyo spent an estimated \$30 million on chemical weapons development, and possessed a number of competent scientists in its ranks. Nevertheless, its use of chemical agents in attacks proved much less destructive than the group had hoped. Some analysts argue that Aum Shinrikyo's use of chemical weapons was an unusual preoccupation related to its idiosyncratic religious beliefs, and that most political terrorist organizations with equivalent resources would choose to pursue conventional attacks for decreased risk and greater return on investment.

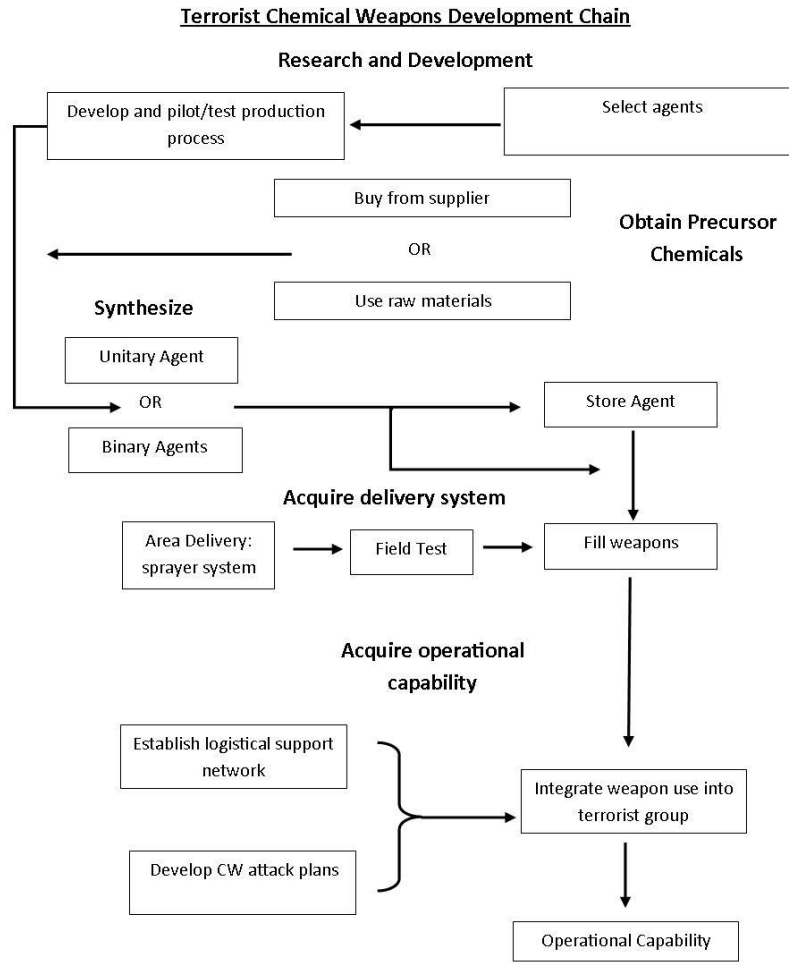
manpower costs of compulsory decontamination of high density urban areas can be high.

Chemical attacks by terrorists and terrorist organizations have been extremely rare internationally and domestically, and have usually been low in lethality due to the difficulty of deploying to lethal concentrations. Nonetheless, effective dispersal of military-grade agents, or successful sabotage of a chemical plant in a major industrial area, could realistically result in massive casualties.

Potential Energy Sector Impacts: *Slight.* With the exception of relatively few high-persistence military-grade agents and dispersal systems currently believed to be possessed exclusively by nation-states, chemical weapons are unattractive for use against energy infrastructure by terrorist organizations, and terrorist organizations capable of acquiring/developing, and then effectively deploying chemical weapons are relatively few in number. Few terrorist organizations have seriously pursued acquisition of chemical weapons, but extremist religious groups may have disproportionate interest in chemical weapons. However, most terrorist organizations which have pursued chemical weapons development, have demonstrated particular interest in targeting civilians in population-dense areas, rather than utilizing chemicals for utility infrastructure attack. Specific targeting of energy sector facilities or infrastructure with chemical weapons appears unlikely. Attacks against energy sector operators utilizing toxic chemicals would likely target personnel and personnel-dense facilities, with area-denial and decreased serviceability as potential secondary objectives. Chemical weapons are not capable of seriously damaging infrastructure components, but persistent agents may render infrastructure unserviceable by unprotected personnel until decontamination is completed. In all cases, the primary hazard of chemical weapons to energy infrastructure operators is to personnel, rather than critical components.

Lethal Chemical Agents by Category			
Category	Mechanism of Action	Time to Onset of Symptoms*	Persistency
Nerve	Interrupts breakdown of the neurotransmitter acetylcholine, leading to central nervous system disruption	Vapor: Very Rapid (>5 minutes) Skin: Moderate (2-18 hours)	VX for military manufacture is a persistent contact hazard and may be treated with thickeners to increase area denial impacts. Most other nerve agents are non-persistent and present an inhalation hazard only.
Asphyxiant/Blood	Deprive the body of oxygen through damaging red blood cells or disrupting cellular metabolism of oxygen	Vapor: Very Rapid (<2 minutes) Ingested: Very Rapid (<2 minutes)	Non-persistent; an inhalation and ingestion hazard only
Vesicant/Blister	Attacks skin, eyes, mucosal membranes, and respiratory system through chemical production of acid burns and blistering	Vapor: Moderate (4-6 hours, with eyes and respiratory system impacted more rapidly) Skin: Moderate (2-48 hours) *the onset times listed above are for Mustards. Lewisite can present very rapidly*	Persistent, constitutes and inhalation and contact hazard. May remain a contact hazard after the inhalation hazard has passed. May be treated with thickeners to increase area denial effects.
Pulmonary/Choking	Similar to vesicants but with more acute impacts to the respiratory system	Vapor: Very Rapid (immediate)	Non-persistent; an inhalation hazard.

*Time to onset of symptoms may vary with time to absorption of lethal or incapacitating dose. Most military doctrine on the employment of chemical weapons recommends dispersal concentrations high enough to produce fatal impacts within seconds of inhalation exposure. Terrorist attacks utilizing chemical weapons have rarely reached such high concentrations



Source: Dana A. Shea and Frank Gottron, "Small-scale Terrorist-Attacks Using Chemical and Biological Agents: An Assessment Framework and Preliminary Comparisons." CRS Report for Congress May 2004

Biological Attack

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
Global/National	Catastrophic	Extremely Rare	Extremely Rare	Moderate	55.00

General Summary: Biological Attack refers to the use of infectious biological agents and toxins like bacteria, viruses, and fungi to kill or incapacitate living organisms. Biological weapons may be applied against personnel, livestock, or crops, and high persistence agents may produce area denial effects that require compulsive quarantines and decontamination before an area or population can be serviced. There is a wide range of weapon-izable biological agents. Most biological warfare agents occur in nature, and are optimized in laboratory environments for dispersal. The effectiveness of biological agents in producing incapacitation among a population is dependent on infectivity, virulence, persistence, and countermeasure availability. Infectivity refers to the biological agent's ability to establish an infection across multiple hosts. Virulence refers to the agent's ability to cause disease in the host once infection is established. Persistence refers to a biological agent's ability to survive and maintain infectivity under storage, transport, or when released into an environment. Pre and post-attack countermeasures may include disruption of plots, prophylactic or reactive vaccination, anti-bacterial or anti-viral medications and treatments, protective gear and quarantine, and epidemiological information-sharing that allows more rapid monitoring and tracking of potential pandemics and biological attacks.

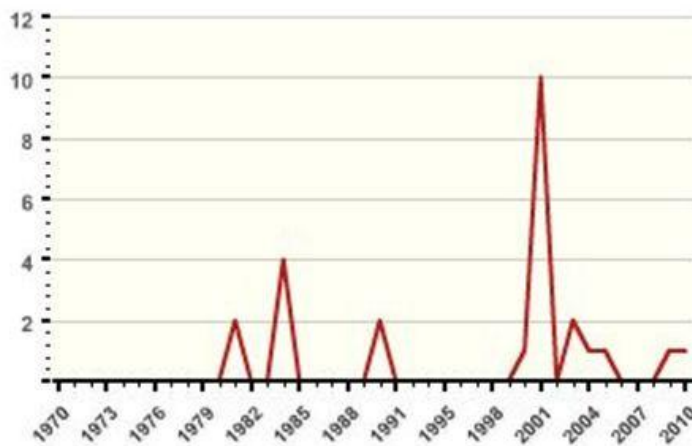
Advanced biological weapons have generally been a Nation-State asset, but some non-state actors have shown interest and capabilities in developing and deploying biological weapons. The United States and Soviet Union engaged in substantial bio-weapons research and development during the Cold War period. The Soviet Union, in particular, focused its efforts on maximization of bio-weapon lethality and infectivity to personnel through genetic augmentation of naturally-occurring biological agents, while the United States focused primarily on bio-weapons defense and anti-agriculture/anti-livestock agents, but also developed significant offensive capabilities before suspending offensive bio-weapons research upon signing the Biological Weapons Convention. Biological weapons development is now largely prohibited under the Biological Weapons Convention, which has 165 signatories including the United States, Russia, China, and India. Notably, the Soviet Union continued to develop genetically engineered offensive weapons subsequent to signing the Biological Weapons Convention, but now appears to have suspended most or all of its offensive bio-weapons research and development. In most signatory states, biological weapons stockpiles are either in long-term storage, or have been eliminated. There are 23 nation-states that are not signatories. With some exceptions, most non-signatory states lack substantial biological weapons development programs and delivery capabilities.

The technological prerequisites to biological weapons development vary considerably depending on agent selected and intended use. Some agents require highly advanced laboratory environments and industrial production facilities, while others can be developed in a low-tech environment. The primary technical obstacle to biological weapons development is not the culturing and development of a dangerous biological agent, but in rendering the agent suitable for weapons use, and transporting and deploying the weapon effectively.

Nation-States have employed biological agents prior to the Biological Weapons Convention. Japan used biological weapons in China during the Second Sino-Japanese War during the World War II period, and the United States deployed biological defoliants during the Vietnam War. During World War I, German agents were apprehended attempting to infect US livestock with biological agents. Defoliant toxins and anti-livestock agents have been utilized in several other counter-insurgencies and civil conflicts before and during the Cold War period. In recent decades, terrorist organizations and individuals have deployed or attempted to develop biological weapons with limited success.

In 1984, followers of the religious cult of Bhagwan Shree Rajneesh poisoned ten salad bars in Wasco County, Oregon with salmonella, in hopes of incapacitating enough voters to ensure the success of their associates in upcoming elections. 751 citizens contracted salmonellosis, but no

Biological Attacks Worldwide: 1970-2010



Source: Global Terrorism Database, 2012

cases were fatal. In 2002, a series of letters tainted with anthrax were sent to the offices of news media and US senators, killing five and infecting seventeen. After an extended and complex investigation, the FBI concluded that the sole culprit for the attack was Bruce Ivins, a senior researcher at the US Army Medical Research Institute of Infectious Diseases at Fort Detrick, Maryland. Ivins was alleged to have stolen bio-weapons materials from his own laboratory, but forensic analysis of the agents used in the attack were unable to conclusively link the attack strain

to the laboratory strain. Ivins is now deceased, and was never formally charged. Al-Qaeda affiliates like Al-Qaeda in the Land of the Islamic Mahgreb (AQLIM) have demonstrated interest in biological weapons development. In 2009, at least 40 Islamic militants associated with AQLIM were reportedly killed by accidental release of pneumonic plague bacteria at a clandestine laboratory in Algeria. The militant base was subsequently quarantined and sealed.

Nation-States have maintained bio-weapons capability both as a first strike and deterrent tool. Biological agents with high infectivity and virulence in humans may be unattractive as an offensive weapon for rational nation-states and non-state actors. High infectivity and virulence can result in uncontrolled spread of communicable diseases to non-target populations, and some biological agents cannot be used on dense populations without the potential for indiscriminate regional or global pandemic. Some biological agents are selected for latency, that is, a period between infection and symptom formation. Many biological agents have a significant latency period, with some taking days or weeks to develop symptoms. Latency periods render many biological agents unattractive as battlefield weapons, but increase the likelihood of casualties and rapid geographic spread if employed against civilian populations.

Since World War II, biological weapons have rarely been used, and use has been limited primarily to non-state actors, or state actors embroiled in civil war or counter-insurgency operations. Between 1970 and 2010, twenty five incidents of biological attack or release by non-state actors have been reported. Biological weapons have been attractive to some terrorist groups and militant organizations. Extremist or apocalyptic militant organizations appear more interested than exclusively political terrorist organizations, in the development of weapons of mass destruction. Under ideal deployment conditions, some biological agents may in fact prove more lethal and disruptive in practice than chemical or nuclear weapons, and therefore represent an opportunity for militant groups seeking mass casualties, panic, and high recovery cost. The ability of some high latency agents to produce rapidly spreading outbreaks of communicable disease, or to enable clandestine release of biological agents and subsequent evasion of law enforcement, may in part explain the apparently higher appeal of biological warfare agents to extremist religious groups than to other types of state or non-state actor, as extremist religious groups tend to be less restrained in seeking higher casualty events. However, the challenges of clandestinely acquiring, weapon-izing, transporting, and deploying biological agents for mass casualties can be considerable, and the twenty five listed terrorist attacks - from 1970-2010 - utilizing biological agents, have cumulatively killed only nine individuals unaffiliated with the plots themselves.

Potential Impacts: Impacts of biological attack are dependent on a series of complex factors. Agent selected for use, quality and weapon-ization of agent selected for use, dispersal method, weather, early warning, and health care and emergency management response can all affect the level of impact brought by biological attack. A "worst case scenario" in which a highly infectious, virulent, and persistent agent with high fatality rates were introduced to a major population via effective dispersal devices, could produce extreme human or animal casualties, require large-scale quarantines and health sector response, and may escape initial quarantine areas to cause secondary outbreaks in other locations.

Potential Energy Sector Impacts: *Moderate.* Like chemical agents, biological agents cannot damage infrastructure directly, but in "worst case scenario" can have catastrophic anti-personnel

or anti-livestock impacts with secondary impacts as a result. Potential anti-personnel impacts include compulsory costs of quarantine, protective equipment, prophylaxis, medical treatment, and decreased staffing capabilities resulting in lost productivity. High persistence agents may produce area-denial impacts requiring compulsory decontamination before an area or population can be serviced. The geographically dispersed nature of energy infrastructure render biological weapons unattractive for direct infrastructure attack, with impacts to energy delivery primarily being a result of potential staffing issues, staff treatment costs, lost productivity, and in less-likely cases, compulsory decontamination of impacted facilities. Unless a hostile actor took unusual initiative in deliberately targeting energy sector operators for sophisticated biological attack, it is unlikely that energy sector impacts in the case of a biological attack would be greater than general impacts to the public or other personnel-intensive and geographically-dispersed critical infrastructural sectors like transportation, government services, or health-care.

Disease	Transmit Man to Man	Latency Period	Illness Duration	Lethality	Persistence of Organism	Vaccine Efficacy (aerosol exposure)
Inhalation anthrax	No	1-6 days	3-5 days (usually fatal if untreated)	High	Very stable, spores remain viable for >40 years in soil	2 doses efficacy against up to 1,000 LD ₅₀ in monkeys
Brucellosis	No	5-60 days (usually 1-2 months)	Weeks to months	<5% untreated	Very stable	No vaccine
Cholera	Rare	4 hours-5 days (usually 2-3 days)	>1 week	Low with treatment, high without	Unstable in aerosols & fresh water; stable in salt water	No data on aerosol
Glanders	Low	10-14 days via aerosol	Death in 7-10 days in septicemic form	>50%	Very stable	No vaccine
Pneumonic Plague	High	2-3 days	1-6 days (usually fatal)	High unless treated within 12-24 hours	For up to 1 year in soil; 270 days in live tissue	3 doses not protective against 118 LD ₅₀ in monkeys
Tularemia	No	2-10 days (average 3-5)	>2 weeks	Moderate if untreated	For months in most soil or other media	80% protection against 1-10 LD ₅₀
Q Fever	Rare	10-40 days	2-14 days	Very low	For months on wood and sand	94% protection against 3,500 LD ₅₀ in guinea pigs
Smallpox	High	7-17 days	4 weeks	High to Moderate	Very stable	Vaccine protects against large doses in primates
Venezuelan Equine Encephalitis	Low	2-6 days	Days to weeks	Low	Relatively unstable	TC 83 protects against 30-500 LD ₅₀ in hamsters
Viral Hemorrhagic Fevers	Moderate	4-21 days	Death between 7-16 days	High for Zaire strain, moderate with Sudan	Relatively unstable: depends on agent	No vaccine
Botulism	No	1-5 days	Death in 24-72 hours; lasts months if not lethal	High without respiratory support	For weeks in nonmoving water and food	3 dose efficacy 100% against 25-250 LD ₅₀
Staph Enterotoxin B	No	3-12 hours after inhalation	Hours	<1%	Resistant to freezing	No vaccine
Ricin	No	18-24 hours	Days- death within 10-12 days for ingestion	High	Stable	No vaccine
T-2 Mycotoxins	No	2-4 hours	Days to months	Moderate	For years at room temperature	No vaccine

Data from the USAMRIID Medical Management of Biological Casualties Handbook, 4th Edition 2001

Physical Attack

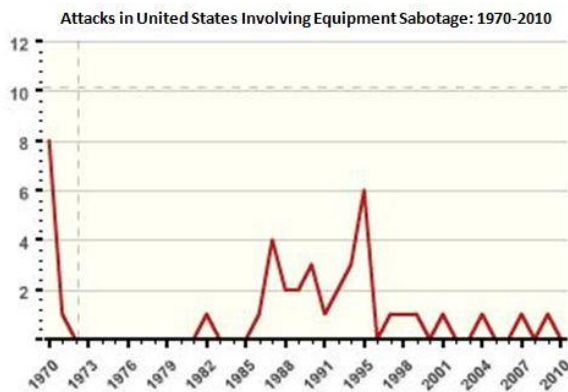
Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
Localized/US-Regional	Moderate	Regular	Very Likely	Moderate	60.83

General Summary: Physical Attack refers to attacks on assets or personnel utilizing sabotage or man-portable weaponry. Sabotage has long been a method of asymmetric warfare utilized by guerillas, activist groups, terrorist organizations, and infrequently by lone individuals, and involves the physical damage, destruction, or disruption of infrastructure components and facilities. Depending on the target selected and desired impacts, a wide variety of tools and methods may be used by saboteurs. Physical attack involving man-portable weaponry may focus on personnel, or in some cases, on components and materiel. Man-portable weaponry favored by potential adversaries may include small arms, anti-materiel rifles, incendiary devices or accelerants, bladed weapons, incapacitating agents, and a variety of other non-explosive weapons.



Arson has been a favored method of physical attack by environmental extremist groups. In 1999, individuals affiliated with the Earth Liberation Front burned several buildings at the Colorado's Vail Ski Resort. The Vail arson caused over \$12 million in damage. Upon apprehension, the perpetrators of the Vail arson later pled guilty to a campaign of environmentally-motivated arsons from 1996-2001, totaling over \$20 million dollars in damage.

In the United States, sabotage has typically been engaged in clandestinely, with its perpetrators attempting to evade law enforcement, whereas physical attackers may or may not expect to evade law enforcement, and are more likely overall to barricade, take hostages or threaten sabotage, fight law enforcement and civilians, or otherwise forego serious attempts at evasion or clandestinity during or after their attack. The combination of physical attacks to commandeer a facility and the threatened or actual carrying-out of sabotage

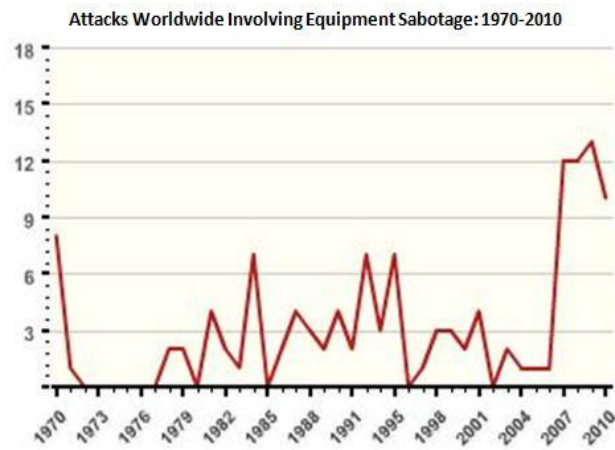


Source: Global Terrorism Database, 2012

at the commandeered facility, remains a possibility and has occurred infrequently abroad. Physical attack or sabotage may intentionally target civilians and intend for maximum casualties, or may be intentionally limited in scope and designed to inflict damage or disruption to targeted infrastructure without resulting in human casualties. The specific approach to physical attack and sabotage is

highly dependent on the identity and intentions of the perpetrating organization or individual.

Sabotage in the United States has been rare, and has declined overall since it first spiked in the early 1970s, and spiked again in the mid-1980 through mid-1990. Sabotage against critical infrastructure in the United States has focused on utilities, telecommunications, and transportation. Left-wing and environmental organizations have tended to focus on telecommunications and utilities, with favored methods being disassembly or destruction of components using tools, equipment, or vehicles, and arson. Sabotage by left-wing and environmental groups in the United States has generally been low casualty or no-casualty, and the targeting and attack methods of environmental groups in the United States appear to reflect an interest in maximizing symbolic or physical impact, while limiting human casualties. Of course, nothing precludes a more militant environmental terrorist group from developing a desire to cause substantial human casualties in the future, but while environmental groups in the United States are among the most common perpetrators of utility infrastructure sabotage, they have not produced significant utility disruption or human casualties from 1970 to 2012.



Source: Global Terrorism Database, 2012



Anti-Materiel rifles like the Barrett M90 shown here are capable of seriously damaging or destroying grid components from approximately 2000 yards. A coordinated attack utilizing anti-materiel rifles simultaneously at multiple critical locations would have the potential to cause substantial disruption to energy infrastructure. Anti-materiel rifles, though relatively costly, are available in civilian and black markets. Fortunately, rifles of this type have very rarely been used for criminal or terroristic violence in the United States.

Right-wing extremist groups have also engaged in sabotage and physical attack against critical infrastructure, but have tended to focus on law enforcement, government facilities, and transportation systems. Though right-wing extremist organizations and sympathizers have not often been successful at physical attacks on infrastructure, their target selections and attack methods have been more likely to cause human casualties. Unlike environmental extremist groups, right wing and religious extremist organizations appear to select targets for greater human casualties.

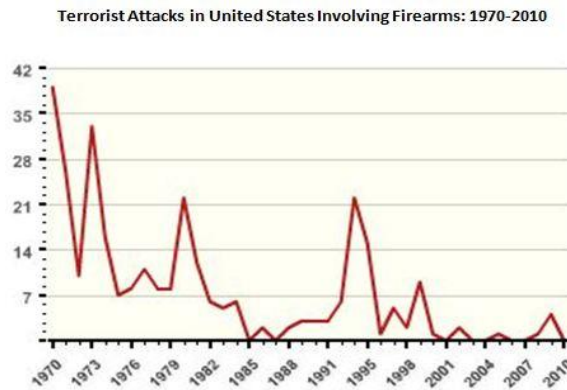
As might be expected, environmental organizations have tended to select targets and methods that avoid catastrophic environmental

damage, however, the potential for a militant religious group or other apocalyptic organization to cause large scale environmental damage through methods like pipeline sabotage remains a concern.

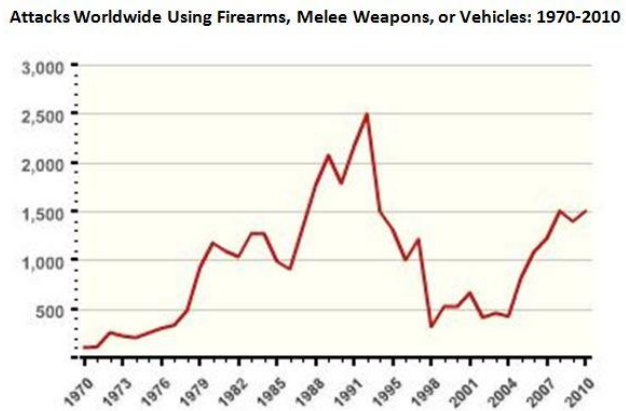
Less frequently, professional criminal organizations may threaten or carry out sabotage as a method of extortion, but physical attack on critical infrastructural facilities or personnel by professional criminal organizations would be highly unusual. Likewise, smaller scale physical attack is sometimes carried out in the form of workplace violence by disgruntled employees or disturbed individuals, but an attack of this type would be more likely to target personnel rather than critical infrastructural assets.

Potential Impacts: Any accessible component, facility, or employee/associate, may be sabotaged or physically attacked. Sabotage and physical attack may be sophisticated and reflect highly specialized knowledge of facilities and systems attacked, or may be opportunistic and hastily planned. Arson can destroy facilities, vehicles, infrastructure components, and other assets. Well-coordinated physical attack by a trained and determined adversaries utilizing small arms, has the potential to produce moderate to severe, but localized casualties and disruption. Well-coordinated physical attack utilizing anti-materiel rifles can damage and disrupt telecommunications and utilities components and disable vehicles. Physical attack targeting critical infrastructure operator executives or personnel have the potential to cause significant disruption to the affected operator/s, but would be unlikely to result in systemic impacts unless combined with additional sabotage or attack methods.

Potential Energy Sector Impacts: *Moderate.* Forms of physical attack intended to maximize casualties, like assault with small arms, are not attractive for application against physically dispersed energy infrastructure and facilities, except as a prelude to sabotage or as part of a casualty-maximizing, rather than infrastructure-disrupting operation. A competent and



Source: Global Terrorism Database, 2012

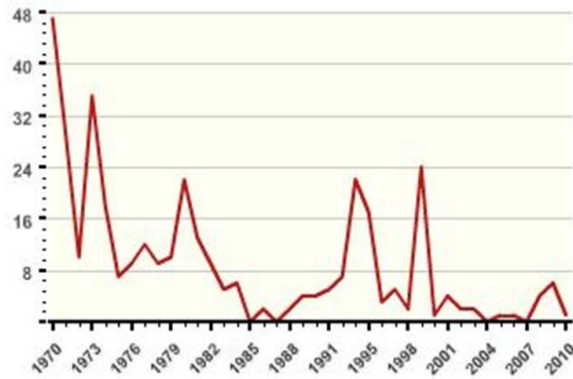


Source: Global Terrorism Database, 2012

knowledgeable adversary organization utilizing anti-materiel rifles or incendiary devices could strategically damage and destroy grid components while at least temporarily evading law enforcement, causing significant disruption to energy sector operations within the State of Colorado. A "worst case scenario" involving physical attack and sabotage of hydroelectric facilities, pipelines, liquid fuels storage facilities, or nuclear facilities, could result in substantial human casualties and very costly environmental and economic impacts.

Fortunately, such a scenario falls beyond the capabilities or intentions of most domestic militant organizations within the United States, and would be difficult to clandestinely plan and carry out without challenge from security personnel or law enforcement. Nevertheless, a competent and well-coordinated adversary might be capable of causing significant disruption via physical attack, sabotage, or a combination of the two methods.

Attacks Within United States Using Firearms, Melee Weapons, or Vehicles: 1970-2010



Source: Global Terrorism Database, 2012

Cyber Attack

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
Localized/National	Severe	Rare	Moderately Likely	Catastrophic-Systemic	84.41

General Summary: Cyber Attack refers to the intentional breach or exploitation of information technology networks and systems in order to cause damage or disruption. Virtually all critical infrastructure sectors rely heavily on networked IT systems to monitor and coordinate operations. Modern energy delivery systems utilize a variety of networked components: Supervisory Control and Data Acquisition (SCADA) Systems enable centralized monitoring and control of energy transport and delivery processes and components. Energy Management Systems (EMSs) are a variety of applications that monitor and optimize performance in energy generation and transmission systems, and are often attached to SCADA systems as an energy systems-specific application suite. Distributed Control Systems (DCSs) are control systems in which controller elements are decentralized throughout the physical infrastructure, and are heavily networked for communication and monitoring. Programmable Logic Controllers (PLCs) are microprocessor based devices which control automated processes and machinery. Intelligent Electronic Devices (IEDs) are microprocessor based devices which control power system

Categories of Adversaries to Information Systems

Adversary	Description
Nation States	State-run, well organized and financed. Use foreign service agents to gather classified or critical information from countries viewed as hostile or as having an economic, military or a political advantage.
Hackers	A group of individuals (e.g., hackers, phreakers, crackers, trashers, and pirates) who attack networks and systems seeking to exploit the vulnerabilities in operating systems or other flaws
Terrorists/ Cyberterrorists	Individuals or groups operating domestically or internationally who represent various terrorist or extremist groups that use violence or the threat of violence to incite fear with the intention of coercing or intimidating governments or societies into succumbing to their demands
Organized Crime	Coordinated criminal activities including gambling, racketeering, narcotics trafficking, and many others. An organized and well-financed criminal organization
Other Criminal Elements	Another facet of the criminal community, which is normally not well organized or financed. Normally consists of few individuals, or of one individual acting alone.
Industrial Competitors	Foreign and domestic corporations operating in a competitive market and often engaged in the illegal gathering of information from competitors or foreign governments in the form of corporate espionage
Disgruntled Employees	Angry, dissatisfied individuals with the potential to inflict harm on the Smart Grid network or related systems. This can represent an insider threat depending on the current state of the individual's employment and access to the systems
Careless or poorly trained employees	Those users who, either through lack of training, lack of concern, or lack of attentiveness pose a threat to Smart Grid systems. This is another example of an insider threat or adversary

Source: *Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements NISTR 7628, volume 1, pp20*

components like circuit breakers, transformers, and capacitor banks. A Remote Terminal Unit (RTU) is a microprocessor based device which interfaces with SCADA or other control systems to transmit telemetry data to the control system, and receive commands from the control system which it then relays to physical infrastructure components.

While the increased networking of energy generation, transport, and distribution systems has produced substantial increases in efficiency, reliability, and real-time monitoring and control, these advances may also introduce a series of vulnerabilities to disruption via cyber attack. Critical infrastructural vulnerabilities may also overlap between businesses IT systems. For example, an operator's financial accounting or inventory management system may be less secure than critical infrastructure control systems, and if the systems are networked, an adversary may be able to exploit access to the less secure system, to gain backdoor access to the more secure system. Dispersed employee access to IT systems through smart phones and other wireless devices, increases the potential for an adversary to exploit points of access.

A variety of actors may attempt to exploit IT security vulnerabilities. Nation-States are increasingly focusing resources on developing cyber-warfare capabilities. Russia, China, North Korea, Israel, Iran, and the United States, among others, have all systematically pursued cyber-warfare and cyber-defense capabilities, with purpose-built units and cyber-commands. A variety of non-state actors, organizations, and individuals may also present as cyber adversaries.

Terrorist organizations have shown interest in developing concrete cyber-attack capability, but terrorist and terrorist-sympathizer exploitation of IT systems and vulnerabilities have primarily revolved around the leveraging of information technology to enable clandestine communications and recruitment, and to gain unauthorized access to information when possible. However, sophisticated terrorist organizations, particularly those with an element of state-sponsorship, are certainly capable of less-sophisticated attacks like Distributed Denial of Service (DDOS), and



While cyber-attacks capable of seriously disrupting energy infrastructure operations have been comparatively rare, a highly sophisticated and well-coordinated attack targeting control and monitoring systems could result in systemic disruption within and between the energy sector and other critical infrastructure sectors. In 2009, a 900 ton turbine at Russia's Sayano-Shushenskaya hydroelectric plant was ripped from its frame due to a rapid water pressure increase combined with a faulty vibration sensor which did not report the danger to the monitoring system. The sudden loss of the turbine resulted in a subsequent transformer explosion and serious damage to the facility. Seventy-five were killed in the accident, prices rose across the Russian energy market, and rebuilding is estimated to cost \$1.3 billion.

While not a case of cyber-attack, the type of failure and resulting damage experienced in the Sayano-Shushenskaya Accident may be indicative of potential results of serious cyber-attack on industrial facilities in the United States. A highly sophisticated cyber-attack might produce similar impacts simultaneously across multiple critical infrastructural sectors and geographic regions.

have demonstrated interest in more serious offensive cyber capabilities.

Exploitation of infrastructure operator IT security vulnerabilities by domestic, or, more frequently, foreign competitors is not uncommon. When corporate intelligence and security specialists contracted by competitor organizations attempt to secure unauthorized access to sensitive or proprietary information at a target company, their actions cross over from legitimate business intelligence and security operations, into criminal industrial espionage. Likewise, nation-state intelligence services have occasionally been discovered engaging in corporate espionage to the benefit of their respective countries' domestic industries.

Hackers are private individuals who seek to exploit vulnerabilities in IT systems often for financial gain, thrills, curiosity, political activism, or reputation. Hackers range in competence between unsophisticated "script kiddies" who are not capable of writing their own malicious code, but who can utilize code written by others, to highly sophisticated "Grey Hat" and "Black Hat" hackers whose training and background rival the best "White Hat" IT security specialists. Hackers often act alone, but may form loosely coordinated organizations and affinity groups capable of engaging in coordinated penetrations. "Anonymous" is a contemporary example of a loosely-coordinated group of hackers capable of successfully engaging in data theft and disclosure as well as larger-scale simultaneously-coordinated DDOS attacks.

Organized crime penetrates IT security for financial gain, or in limited circumstances, to gain access to or alter information. Hackers affiliated with criminal syndicates have targeted business data, customer data, financial records, research data, law enforcement data, inventory management systems, and other potentially valuable information for exploitation or sale. Criminal

Insider Threats: Real Vulnerabilities and Simple Countermeasures

Some of the most serious potential security vulnerabilities involve inside access to IT systems rather than a more ambitious and technically challenging breach from outside the system.

The problem may originate with employees intentionally breaching IT systems to blackmail and extort the company for money, privileges, or job security, to steal from the company, to cover-up embezzlement or other wrongdoing, or may be intended to penalize the company for a perceived slight. Likewise, employees must be trained to vigilantly follow information security guidelines, or they may be vulnerable to "human engineering," a type of internal or external breach intended to exploit employees' natural willingness to inadvertently share critical security information.

Many of the most damaging cases of "hacking" have required little technical capability due to the effectiveness of human engineering combined with basic IT penetration testing and intelligence collection techniques in gaining the prerequisite information necessary to simply log into a critical system through designated access points using genuine credentials.

Fortunately, countermeasures to these kinds of insider threats often do not require major expenditure on additional IT security technologies, but can be addressed cost-effectively through appropriate security procedures, training, redundancy, and access management.

Con't...

In February 2010, over 100 automobiles in the Austin area suddenly stopped functioning, locked out their owners, or began uncontrolled honking. The problem was attributed to the actions of a disgruntled dealership employee who learned a co-worker's login information for the dealership's vehicle monitoring software. The employee also caused serious disruption to the dealership's financial and inventory records using the co-worker's administrative privileges.

In July 2008, many public sector offices in the city of San Francisco ground to a standstill, as the city's networked computer system had administratively locked out all users. The lockout was attributed to Terry Childs, a disgruntled city computer engineer who had designed the city administration IT networks, and possessed sole knowledge of the passwords necessary to end the lockout. Childs was arrested, but would not reveal his administrative passwords. The City of San Francisco promptly spent \$1.5 million dollars in an unsuccessful attempt to break into the network via brute force attack and backdooring. Eventually, Childs revealed the passwords after receiving the personal visit from the mayor that he demanded.

On July 30, 1996, employees at Omega Engineering, a defense contracting and design firm, were shocked to discover that more than a thousand crucial design and production programs as well as virtually all essential company records, had been deleted. Backup records were also found to have been wiped. The culprit was rogue programmer Timothy Lloyd, who had leveraged his administrative privileges to inject malicious code into the company's databases, and gained physical access to backup media and clandestinely deleted them. Lloyd planned and orchestrated his attack in anticipation of Omega terminating his employment, and deliberately designed the code to activate *after* he had left the company. The security breach cost Omega more than \$10 million, and was a serious blow to the quickly-growing company.

syndicates and affiliated hackers may also be contracted by nation-states for smaller-scale or less-sophisticated cyber attacks. Criminal hackers can sometimes be differentiated from activist hackers based on target selection, sophistication, and type of attack. Activist hackers may select targets they specifically wish to embarrass or damage, and steal data for public disclosure. Criminal actors will typically steal data for disclosure to private black market buyers or internal exploitation, rather than release to media. Information and systems targeted may differ accordingly. A competent independent hacker unaffiliated with any organization, may be capable of significant data theft and unauthorized access, but typically will not have an extended network of accomplices capable of physically accessing or exploiting facilities utilizing stolen data. Conversely, a criminal or terrorist organization may engage in coordinated physical and cyber operations, for example, physical collection of customer or employee RFID data or credit card data and cloning of cards to gain unauthorized access to facilities or financial accounts, access to databases and control systems to damage infrastructure, and divert or degrade services in conjunction with physical attack or penetration.

Disgruntled employees have occasionally engaged in damaging cyber attacks. Disgruntled employees may breach IT systems for financial gain, personal grievance or dissatisfaction, political activism, or to punish employers for a perceived slight. Employees with "insider" access or specialization in IT security systems may possess all the prerequisites to engage in damaging cyber attacks against an organization. Disgruntled employees may carefully plan their operations in advance, often leveraging information gleaned from well-meaning but careless colleagues who inappropriately disclose seemingly-harmless information about IT systems.

Potential Impacts: Cybercrime, cyber-warfare, and cyber-attack may utilize a wide range of technical

methods, at varying degrees of sophistication and potential impact. While less sophisticated incidents of cybercrime and casual hacking are extremely frequent, sophisticated cyber attacks capable of seriously disrupting critical infrastructure and services have been comparatively rare and could be considered a High Impact/Low Probability (HILP) event. Some of the more serious alleged cases are perpetrators either affiliated with nation-states and sophisticated criminal and "hactivist" organizations or idiosyncratic insider threats by employees.

The cumulative economic impact of criminal data theft is high. In 2009, IT Security firm McAfee surveyed 800 Chief Information Officers at major international companies, and estimated that these companies alone lost \$4 Billion in intellectual property, and spent \$600 million repairing and securing networks after breaches. McAfee estimated that the cumulative impact across the global economy now exceeds \$1 Trillion per year. Confirmed examples of sophisticated infrastructure attack with disruptive impacts are much less frequent, but their potential remains. As with other potentially mass-destructive methods of attack, attribution may be important to deterrence. If an adversary is capable of sophisticated infrastructure attack while remaining anonymous, deterrence is degraded. However, Nation-States are the potential adversary most capable of engaging in serious infrastructure attack, and Nation-States are likewise the most vulnerable to counter-attacks on critical infrastructure, whereas a geographically dispersed clandestine organization like a criminal syndicate or terrorist organization, would not be as vulnerable to deterrence, and may in fact enjoy greater freedom to engage in cyber attack with lower risk. Fortunately, as of this document's publication, few non-state organizations have proved capable or willing to engage in major cyber-attack targeting critical infrastructure.

Virtually all critical infrastructure sectors are dependent on SCADA systems, networked databases, networked communications, and other potentially vulnerable IT systems. SCADA systems are utilized to control processes in water treatment and delivery, energy generation, transport, and distribution, hydroelectric facilities, and pipeline operations. Networked records and databases are critical to public health, finance, essential government services, and law enforcement. Networked tracking, routing, and dispatch systems are critical to transportation, agriculture, emergency management and response, mail service, and commodity delivery. Complex control systems are utilized by a wide range of heavy industries like mining, heavy manufacturing, and refining. Networked shipping/receiving and inventory management systems are essential across many industries. Serious disruption within one sector may produce escalating or cascading failures within and between interdependent critical infrastructure sectors.

Potential Energy Sector Impacts: *Catastrophic-Systemic.* Intrusions into a smart grid system, intelligent electronic device/smart device substation controller, SCADA system, or IED could be as severe as physical sabotage. Pipelines, generating facilities, substations and transformers, and other major components can be severely damaged or destroyed, with secondary impacts distributed across respective networks. A sophisticated cyber attack might target multiple assets

simultaneously for increased disruption, or might combine cyber attack with physical attack. If well-planned, an attack of this sophistication could produce catastrophic-systemic disruptions. For information on cyber attack from an “exercise” perspective, see Book 3 - Risk and Vulnerability Assessment in the Exercises subsection, under Intra-State Exercise – Cyber Attack.

Table X-14 A Selection of High Profile Cyber-Attacks

Attack	Adversary Type	Attack Type	Impacts
Brazil Blackout of 2007	Hackers/Unknown (Unconfirmed)	SCADA/Control Systems	Blackout impacting 3 million in Sao Paulo suburbs
Russia/Georgia War of 2008	Nation-State	SCADA/Control Systems, DDOS attack	Pipeline + fuel delivery disruption during armed conflict, disruption of Georgian government websites and networks
Farewell Dossier Incident of 1982	Nation-State	SCADA	CIA “Logic Bomb” introduced to Soviet SCADA software seriously damages Siberian natural gas pipeline
Stuxnet	Nation-State (Unconfirmed)	SCADA/Control Systems	Well-engineered and narrowly-targeted payload disrupts centrifuge operations for Iranian nuclear materials refinement
April 2009 LOIC Attack	Hackers	DDOS Attack	Members of online hacker group “anonymous” undertake massive coordinated DDOS attack, knocking offline or degrading performance for websites belonging to the US Department of Justice, the FBI, Universal Music Group, the Recording Industry Association of America, and the Motion Picture Association of America
Omega Logic Bomb, 1996	Disgruntled Employee	Malicious Code/Logic Bomb/Physical destruction of backup media	Disgruntled programmer deletes virtually all essential company information, resulting in more than \$10 million in recovery costs
Operation Orchard	Nation-State (Unconfirmed)	Unknown	Israeli cyber-warfare teams allegedly introduce malware payloads to Syrian air defense systems, rendering them ineffective during Israeli over-flight

Electromagnetic Pulse (EMP) Attack

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
National/US-Regional	Catastrophic	None	Extremely Rare	Catastrophic-Systemic	73.33

General Summary: Electromagnetic Pulse (EMP) Attack refers to the generation of powerful bursts of electromagnetic radiation in order to damage or destroy electronic components. Electro-magnetic pulses can be generated via nuclear detonation and by a variety of non-nuclear electro-magnetic generation methods like microwave generators and explosively-pumped flux compression generators. Nuclear EMP weapons are similar in design to traditional nuclear and thermonuclear weapons but may be optimized for electromagnetic pulse generation. Nuclear EMP weapons must be delivered via ballistic missile, and optimized for high altitude detonation. Depending on detonation altitude, High Altitude Electromagnetic Pulse Weapons (HEMP) can disperse multiphase electromagnetic pulses that induce damaging currents that exceed breakdown voltage in conductors, followed by geomagnetically induced currents like those encountered during a Geomagnetic Storm, but likely to be more severe and more widely dispersed. Non-nuclear EMP devices are much more restricted in geographic range, and are not known to have been constructed or acquired by any non-state actor, but their construction and deployment involves significantly lower technological prerequisites than for a nuclear EMP device.

No nation-state officially maintains High Altitude Nuclear EMP weapons, though the United States and Soviet Union first began researching and testing HEMP effects in the early 1960s. It is likely that the United States maintains deployable HEMP capability, and possible that several other nuclear nation-states have deployable HEMP capability, or the potential to develop it. Non-nuclear EMP devices have been developed by most nuclear nation-states, and



EMP AREA BY BURSTS AT 30, 120 and 300 MILES

Gary Smith, "Electromagnetic Pulse Threats", testimony to House National Security Committee on July 16, 1997

might theoretically be constructed by sophisticated non-state organizations. However, despite the potential attractiveness of EMP to a small number of extremist groups, most militant or criminal organizations would find the costs and technical challenges of clandestine EMP weapon development and deployment to be prohibitive. Even sophisticated non-state actors might

calculate the risks, opportunity costs, and costs to political legitimacy that use of an exotic and highly destructive weapon such as an EMP would entail, to be insufficiently understood to make EMP development a realistic option for most non-state actors. Despite the very low probability of EMP attack by any actor, the potential for catastrophic disruption of virtually all economic and government activity within an extensive geographic range, in the case of Nuclear HEMP, or even within a quite localized geographic range, in the case of Non-nuclear EMP, cannot be entirely discounted due to the potentially extreme scale of impact.

Potential Impacts: Depending on detonation altitude, a HEMP device may damage or disable most unshielded microprocessor-based electronics within an area ranging as wide as 3000 miles in diameter. Depending on design and delivery characteristics, a non-nuclear EMP would have similar impacts over a much more localized area ranging from a few city blocks to an entire metropolitan area, but would not produce geomagnetically induced ground currents.



Non-nuclear EMP devices have been constructed by several nation-states for testing of EMP mitigation measures on critical assets. Though the most potentially destructive forms of High-Altitude Nuclear EMP weapons (HEMP) fall within the technological capabilities of only a few nuclear states, less powerful Non-Nuclear EMP devices may be within the technological reach of a small number of non-state actors. Above: A Boeing E4 Airborne Command Center Aircraft is tested for EMP resistance at a non-nuclear EMP simulator.

Virtually all major critical infrastructure and government operations outside of some military and continuity of government assets and facilities can be severely disrupted by EMP. Road, rail, maritime, and aviation dispatching and control systems would be severely impacted, as would many of the transport vehicles. Industry, finance, healthcare, agriculture, government services, and other critical sectors are heavily dependent on micro-processor based systems, and would be degraded or completely disrupted. Most terrestrial telecommunications assets within the impact area would be disabled, and in the case of HEMP detonation, satellite and microwave communication could be impacted as well.

Potential Energy Sector Impacts: *Catastrophic-Systemic.* All EMP devices induce over voltages in unshielded conductors, and HEMP devices can also produce geomagnetically induced currents analogous to the currents that would be experienced in a severe geomagnetic storm. These currents can damage or destroy transformers and pipeline components. Microprocessor-based monitoring and control systems, as well as business IT systems, would be severely disrupted or rendered non-functional. Failure in other critical infrastructural subsectors like telecommunications, government services, transportation, and finance, could exponentially increase the challenges of recovery. The wide geographic dispersal of severely disruptive impacts in the case of HEMP detonation renders virtually any HEMP detonation a potentially catastrophic-systemic threat. Non-nuclear EMP detonation impacting even a moderately-sized

portion of a major metropolitan area, would produce catastrophic impacts, but would be considerably less likely to result in regional or national systemic failure.

Major Transportation Accident or Disruption

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
Local/Global	Severe	Rare	Rare	Severe	67.08

General Summary: Major transportation disruption refers to significant disruption of passenger or freight transport between locations and transport modes, through natural hazard, intentional act, or accidental cause. Most modern economic activity now relies heavily on complex transportation and logistics systems. Technological developments have revolutionized the speed, safety, and efficiency of passenger and freight transport in recent decades. Complex logistics management systems enable businesses to utilize Just In Time (JIT) delivery, which maximizes returns on investment by reducing carrying costs on in-process or stored inventory.

Sophisticated inventory management systems enable shippers and receivers to streamline and speed up shipping processes with greater precision and decreased loss of inventory in transit. Developments in shipping like intermodal cargo containerization and mechanized loading and unloading processes have rapidly increased the efficiency and volume of domestic, regional, and global trade. Increased efficiency and safety in passenger and freight aviation have contributed significantly to economic development in the US and abroad. Advances in transportation management and technology have increased the role of intermodal transport. Intermodal transport involves the use of multiple modes of transport to deliver passengers or freight. Developments in intermodal transport have increased the average geographic distance between production and consumption of goods, while decreasing costs through economies of scale.

Global Attacks Targeting Aviation, Maritime, Road, or Rail Transport Assets: 1970-2010



Attacks in United States Targeting Aviation, Maritime, Road, or Rail Transport Assets: 1970-2010



Source: Global Terrorism Database, 2012

While advances in efficiency, management, and transportation technology have rapidly increased the scale and scope of global trade, reliance on intermodal transport, JIT shipping, and complex routing and dispatching systems can increase the potential for major transportation disruption. Increased scale of transport can increase the scale of impact when major transport routes are disrupted. Intermodal transport facilities can increase the potential for significant casualties or



Increased scale of transport can increase the scale of disruption, particularly when intermodal transport hubs are impacted. For example, one quarter of globally traded goods pass through the Strait of Malacca (pictured above) between Malaysia and Indonesia annually on over 50,000 vessels. The strait narrows at several choke points, one of which is only 1.5 nautical miles wide. Similarly, the Strait of Gibraltar connecting all maritime commerce between the Atlantic and Mediterranean coast, narrows to only 7 miles, and the Strait of Hormuz at the mouth of the Persian Gulf, carries 20% of the world's oil annually and narrows to 21 nautical miles.

Disruption of maritime commerce in any of these strategic chokepoints would substantially increase the costs of energy and goods in the global market. The Strait of Malacca has suffered a high volume of maritime piracy in recent years, but recent naval crackdowns have decreased the incident significantly rate over time. Nevertheless, the potential remains for serious disruption of global shipping if a militant group or other actor were to sabotage a large oil transporter in the Strait's chokepoints.

assets have been attacked by left or right-wing domestic terrorist organizations and militant ethno-nationalist groups as well. No attack on transport sector operators or assets within the US have been optimized for infrastructure disruption, with adversaries tending to concentrate on maximizing civilian casualties, symbolic impact, or media attention.

Natural hazards and accidents may also seriously impact transportation sector operations, but the complexity of the global transport system can also mitigate routine hazards, or hazards with

escalating disruptions because intermodal hubs often locate large volumes of critical assets from multiple transport sub-sectors in one potentially vulnerable location. Just In Time delivery systems increase the potential for retail and wholesale shortages when transport is disrupted. Complex routing systems can be exploited for criminal or terroristic purposes, as transportation assets are utilized to smuggle illicit goods, weapons, or people.

Successful attacks on transportation assets and infrastructure have been rare in the United States, but the 2001 attacks on the World Trade Center and Pentagon made clear the potential destruction that threats or exploitations of the transport sector can cause. In the United States, intentional attacks against transportation assets and infrastructure have declined since their peak in the 1970s, and been periodic and lower volume since the 1990s. A majority of attacks against transport sector operators in the United States have focused on passenger aviation. Al-Qaeda affiliated groups and sympathizers have demonstrated particular interest in both passenger and freight aviation. Less frequently, aviation and rail

localized or even transient regional impacts. Nexuses and interdependencies with other critical infrastructure sectors are common, and resulting vulnerabilities are apparent. Intermodal transportation hubs require telecommunications, energy, and government assets to support transport operations. Serious disruptions to other sectors may degrade transport sector capabilities, and transport disruption can degrade other critical infrastructure sector operations in turn, as well as slow delivery and increase costs of consumer goods, commodities, and energy.

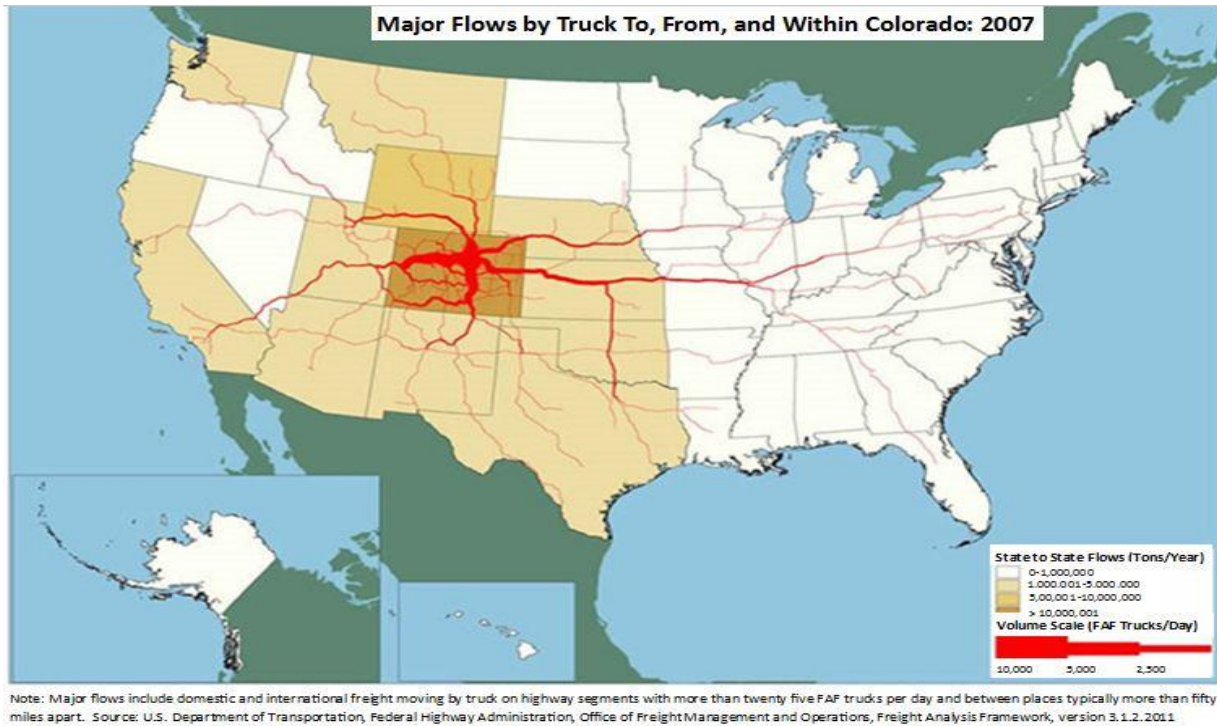
Potential Impacts: In most developed countries, transportation sector operations account for between 6%-12% of gross domestic product. However, cross-sector interdependencies render the true costs of transport disruption more difficult to quantify. Transport disruption can impact the costs and challenges of commodity delivery and personal transportation, severely degrading economic activity in disrupted areas. While transportation sector consolidation and centralized management can increase the costs of disruption, they can also mitigate the impacts of disruption and increase resilience by providing a complex network of transport options which can adapt to transport needs.



Intermodal containerization revolutionized global trade by allowing goods to be packaged for transport in standardized containers that can be transferred between sea, rail, and road vehicles with automated industrial machinery.

As transport systems are first developed, they provide high marginal returns on investment as new geographic areas become accessible. As transportation systems become heavily developed, they provide diminishing marginal returns on investment, but higher efficiencies and greater multi-mode resilience. For example, the heavily developed road transport system in the United States moves commodities less efficiently by weight than rail systems, but disruption of a major rail route will tend to produce greater secondary impacts than disruption of a road route due to the greater number of alternate routes available through the more developed and consolidated road system. Likewise, the US

aviation system is remarkably safe per passenger and freight mile traveled, and compares favorably to road travel, which alone accounts for 90% of property losses and loss of life in US transport. However, the disruptive and economic impacts of a single fatal incident on the road transport system is several orders of magnitude lower than the disruptive impact of a single fatal incident within the more centralized and higher passenger density aviation system.

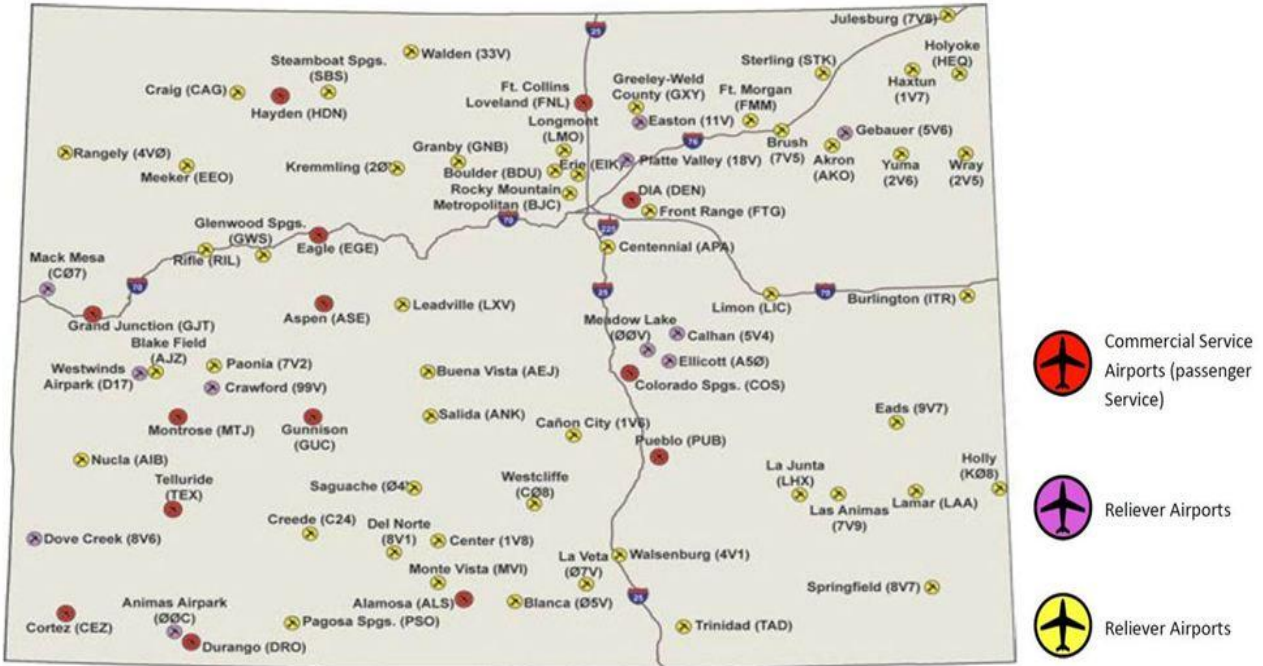


Potential Energy Sector Impacts: Severe. All critical infrastructural sectors are dependent on the transportation sector to varying degrees, and vice versa. Transportation is the most energy-consuming infrastructure in the United States. The majority of the transportation sector's energy consumption is in refined liquid fuels, though increased use of electric road and rail vehicles may increase electrical consumption for transport in the future.

Interdependencies between transportation and energy production are particularly likely to produce escalating or cascading impacts. Refinement of liquid fuels for use by transportation assets is dependent on the transportation of unrefined fuels via pipeline, sea, road, and rail. Medium to long-term disruption of natural gas pipeline or electrical power to natural gas generation facilities can curtail natural gas production, leading to decreased heavy oil production and subsequent degrading of road, rail, and maritime freight transport. Disruption of oil pipelines or power delivery to oil pipelines can lead to decreased production of refined fuels essential for road transport and aviation.

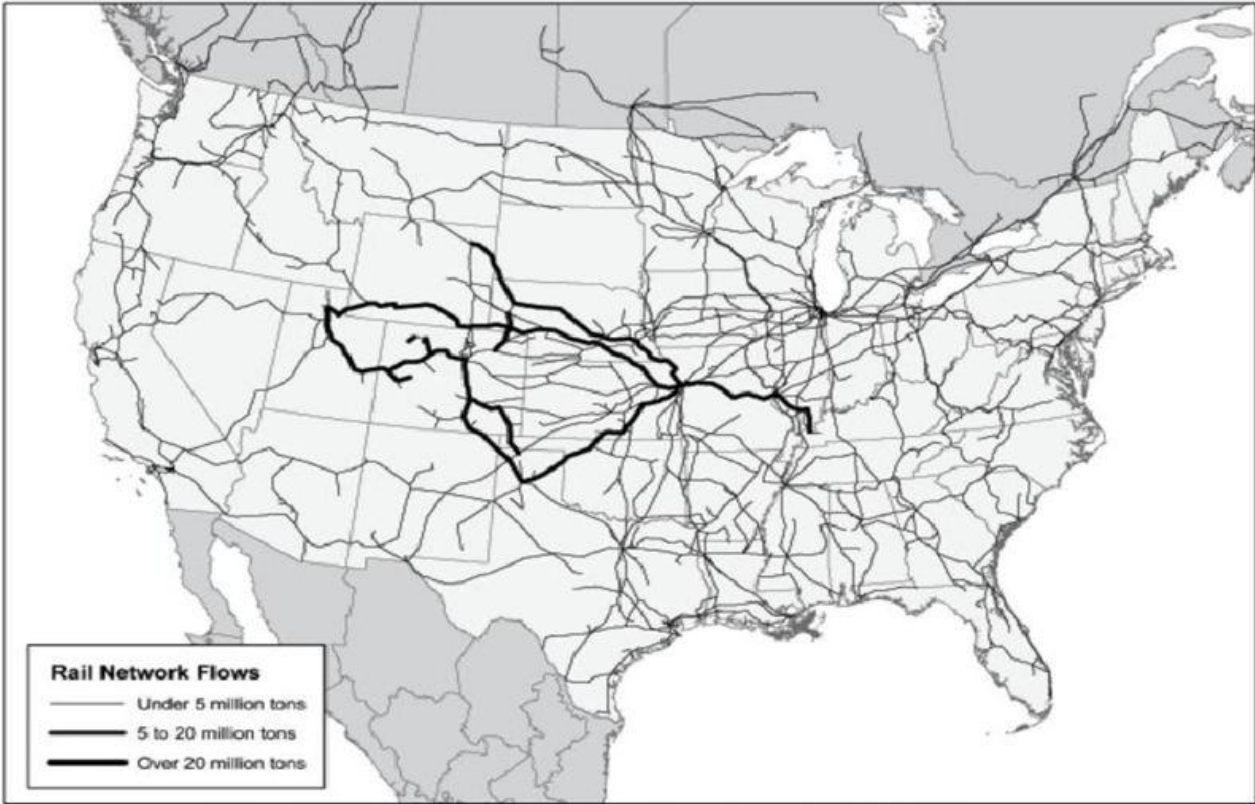
Likewise, major disruption of maritime trade can produce shortages or price spikes in oil and natural gas necessary for electrical generation and liquid fuels refinement. Disruption of rail can produce localized or regionalized shortages of coal and liquid fuels. Disruption of road transport networks can produce localized or regionalized shortages of liquid fuels necessary for road and air transport, and can increase the costs and difficulty of accessing and servicing infrastructure. However, though interdependencies within global and domestic intermodal transportation networks can multiply impacts and produce escalating and cascading effects in the event of

major disruption, the increasing sophistication and consolidation of intermodal transport networks may also mitigate impacts, decreasing the potential for catastrophic-systemic failures in the transportation sector.



Source: CDOT Aeronautics Division, 2010

Interstate Rail Freight Flows to and from Colorado



Source: U.S. Department of Transportation, Federal Railroad Administration, Office of Policy 1999

Dam failure

Geographic Extent	General Impacts	Previous Occurrences	Future Probability	ESIS	RCS
State-Regional/Localized	Severe	Rare	Rare	Severe	53.74

General Summary: Dam failure refers to the uncontrolled release of water from a hydrologic barrier installation due to failure or overtopping. Dam failure may have a variety of causes: Seismic activity or geologic instability can weaken and degrade dam performance, leading to failure, or can trigger rockslides which lead to overtopping. Internal erosion may cause failure, particularly in earthen dams,

and extreme inflow caused by precipitation, upstream flooding, or upstream dam failure, can cause overtopping or failure. Design error, accident, acts of war, or deliberate sabotage via physical means or cyber-attack can also cause dam failure.

Classification of Dams

Classification	Description
Class I - High	Loss of human life is expected.
Class II - Significant	Significant damage is expected, but not loss of human life. Significant damage refers to structural damage where humans live, work, or recreate or public or private facilities exclusive of unpaved roads and picnic areas. Damage refers to making the structures uninhabitable or inoperable.
Class III - Low	Loss of human life and damage to structures and public facilities not expected.
Class IV - No Public Hazard	No loss of human life is expected and damage will only occur to the dam owner's property in the event of dam failure.

Source: Colorado Division of Water Resources

There are over 80,000 dams in the United States. The 2007 National Inventory of Dams assigns a "high" or "significant" risk to life and property safety for one-third of these dams in the event of failure, with "high" risk indicating an expected loss of life upon failure, and "significant" indicating substantial property loss but no expected loss of life upon failure. In Colorado there are approximately 1900 dams, with 677 classified as Class I or Class II.

Dam failures can develop slowly, due to erosion or other geologic factors, or can develop much more rapidly due to extreme inflows, rockslides and seismic activity causing overtopping, structural or equipment failures, or sabotage. Maintenance and management



Remains of the Gleno Dam, which failed due to faulty engineering in 1923.

issues can contribute to dam failures, or increase risk of failure coincident with natural hazards. Dams may be vulnerable to physical sabotage, or may be sabotaged through penetration of SCADA or other control systems to cause failures in spillway gates or turbines. Dams have been deliberately destroyed by military forces in wartime operations in the past, and have rarely been targeted by insurgents abroad, with little apparent success. No deliberate attacks on dams have occurred in the United States as of this writing, but a successful sabotage or explosive attack would likely produce results consistent with rapid structural failure.

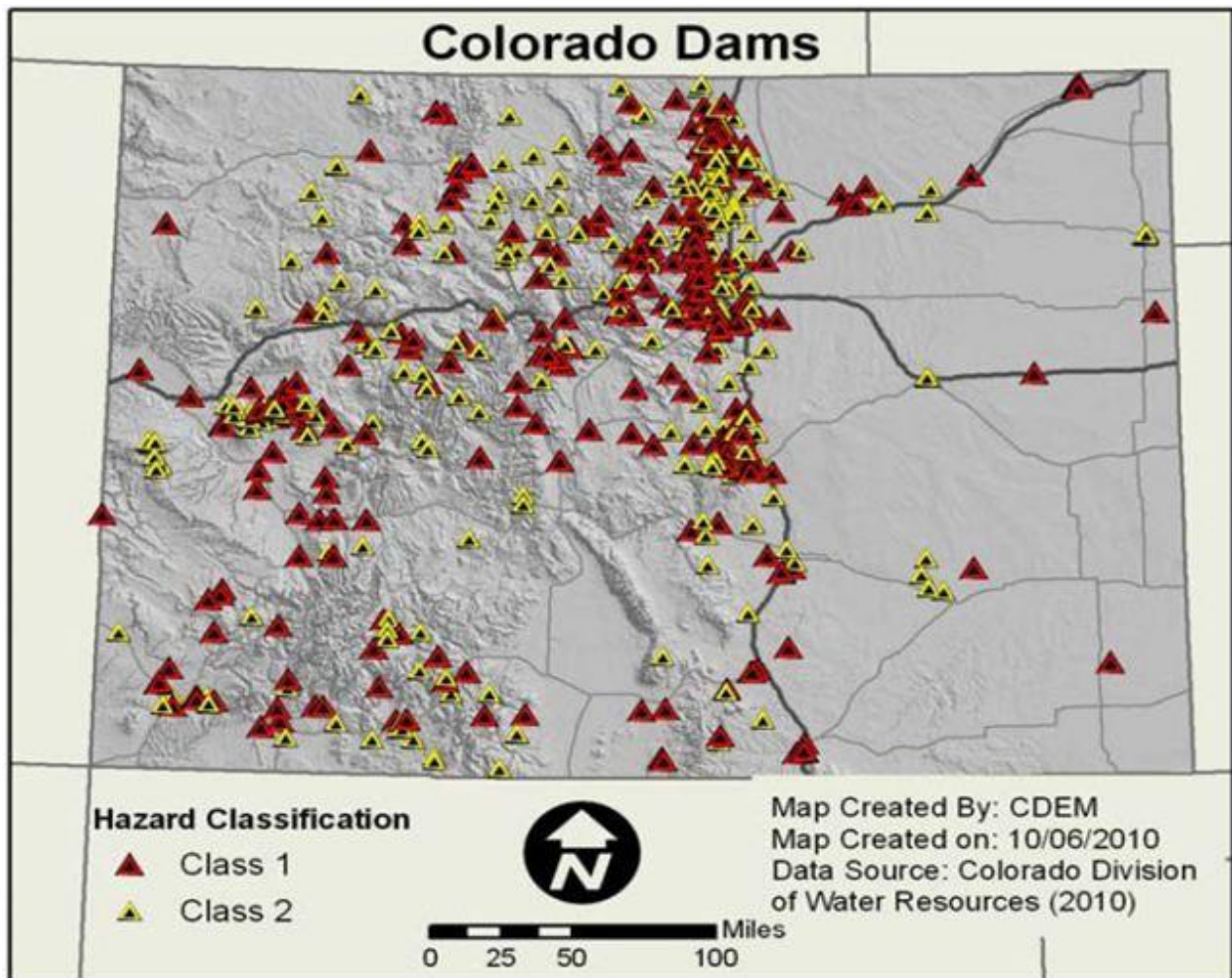
Table X-15 Incidents of Dam Failure and Causal Factors

Incident:	Cause of Failure:	Description:
<i>Gleno Dam Failure Bergamo Italy -1923</i>	Sub-Standard Construction Materials & Techniques	Heavy rains rapidly fill reservoir shortly after construction, leading to failure. Four villages destroyed, 356 killed.
<i>Lawn Lake Dam Failure Rocky Mountain National Park Colorado -1982</i>	Erosion Resulting from Lapsed Maintenance	Unmaintained caulking between outlet pipe and gate valve results in erosion and failure. 3 killed, \$31 million in damages
<i>Upriver Dam Failure Spokane, Washington -1982</i>	Turbine Failure and Subsequent Overtopping of Hydroelectric Dam	Lightning strikes result in unanticipated turbine shutdown. Failure of backup power prevented opening of spillway to alleviate water buildup. 0 killed, \$11 million damage to facility and temporary disruption of generation
<i>Vajont Dam Overtopping Veneto, Italy -1963</i>	Massive Landslide Rapidly Displaces 90% of Reservoir and Subsequent Overtopping	Heavy rains trigger massive landslide and 820 foot wave which empties reservoir without seriously damaging dam. 5 towns destroyed, 1900-2500 killed
<i>Banqiao Hydroelectric Dam Disaster Henan, China -1975</i>	Typhoon Rains Cause Heavy Flooding and Cascading Dam Failures	Heavy upstream flooding caused by record rains leads to cascading failures on smaller upstream dams, resulting in overpressure on larger Banqiao Dam. Spillway gates could not be fully opened due to sediment buildup, and orders to destroy the dam before catastrophic overtopping occurred could not be carried out. 171,000 killed, 11 million homeless, and 18 GW of generating power lost
<i>Sayano-Shushenskaya Hydroelectric Dam Accident</i>	Water Pressure Spike Combined with Faulty Vibration Sensor Results in Serious Facility Damage	A rapid increase in water pressure increased stress on hydroelectric turbines. A faulty vibration sensor failed to alert operators, and a 900-ton turbine was then ripped from its assembly. Sudden loss of the turbine resulted in a transformer explosion and serious damage to the facility. 75 killed, \$1.5 billion rebuilding cost

Potential Impacts: Slowly developing failures can often be mitigated or prevented with sufficient early warning. Rapidly developing failures are typically catastrophic or severe.

Height and speed of resulting floodwaters are dependent on a variety of hydrologic and topographic factors, but have reached hundreds of feet in major disasters when sufficient volumes of uncontrolled water race through narrow topographies. General impacts resemble flash flood, or in some larger scale failures, tsunami waves. Catastrophic failures usually produce severe damage or total destruction to structures and assets as well as high mortality in populated areas of the flood zone.

Potential Energy Sector Impacts: *Severe.* Modern engineering, monitoring and coordinating systems, and maintenance practices minimize the likelihood of rapidly developing catastrophic or cascading failures. However, rapid failure at hydroelectric facilities can compound flooding impacts with loss of generating capacity. Critical energy assets like transmission and distribution lines, and transformers are often located in populated and serviceable valleys that constitute potential dam flooding corridors. Rapid overtopping or failure can produce floods capable of severely damaging or destroying any energy assets in the flood zone.



Source: Colorado Natural Hazards Mitigation Plan

Table X-16 Class I and Class II Dams in Colorado

County	Class I	Class II	County	Class I	Class II
Adams	8	12	Kit Carson	1	0
Alamosa	0	0	La Plata	8	6
Arapahoe	8	4	Lake	3	2
Archuleta	2	8	Larimer	51	40
Baca	1	0	Las Animas	6	1
Bent	2	0	Lincoln	1	2
Boulder	28	21	Logan	3	0
Broomfield	3	1	Mesa	22	29
Chaffee	2	2	Mineral	5	6
Cheyenne	0	0	Moffat	1	3
Clear Creek	8	5	Montezuma	8	7
Conejos	2	3	Montrose	9	1
Costilla	3	1	Morgan	0	6
Crowley	0	2	Otero	0	7
Custer	0	1	Ouray	1	0
Delta	17	13	Park	5	3
Denver	7	3	Phillips	0	0
Dolores	1	2	Pitkin	2	7
Douglas	2	6	Prowers	0	1
Eagle	8	5	Pueblo	3	4
El Paso	18	15	Rio Blanco	3	3
Elbert	0	0	Rio Grange	1	1
Fremont	3	3	Routt	8	5
Garfield	6	11	Saguache	0	1
Gilpin	1	0	San Juan	0	0
Grand	7	2	San Miguel	5	0
Gunnison	6	6	Sedgwick	3	0
Hinsdale	3	4	Summit	5	2
Huerfano	5	3	Teller	4	10
Jackson	0	4	Washington	1	0
Jefferson	22	12	Weld	12	17
Kiowa	0	2	Yuma	1	7

References and Resources

Colorado Energy Assurance Emergency Plan (CEAEP)

References and Resources Table of Contents

Book 1: Overview, Data Collection and Future Progress.....	1
Book 2: Energy Assurance Action Plan.....	3
Book 3: Energy Assurance Risk and Vulnerability Assessment	4
Book 3A: Hazard Typology and Quick Reference GuideTM	13

This Page Intentionally Left Blank

Book 1: Overview, Data Collection and Future Progress

Section IV: Community Profile

“American Recovery and Reinvestment Act of 2009” *The Recovery Act*.

http://www.recovery.gov/about/pages/the_act.aspx

“Climate Action Plan Overview.” *Climate Action Plan Overview*. Colorado Department of Public Health and Environment, 2007.

<http://www.cdph.state.co.us/climate/climateactionplan.html>

“Colorado Energy Office.” <http://www.colorado.gov/energy/>

Colorado: Overview. U.S. Energy Information Administration. October 2009.

<http://www.eia.gov/state/state-energy-profiles.cfm?sid=CO>

“Energy Assurance Guidelines Version 3.1.” *NASEO*. National Association of State Energy Officials. <http://www.naseo.org/eaguidelines/>

Exec. Order No. D 005 05, “Greening of State Government” (2005).

<http://www.colorado.gov/cs/Satellite?blobcol=urldata&blobheadername1=Content-Disposition&blobheadername2=Content-Type&blobheadervalue1=inline%3B+filename%3D%22%2821%29Executive+Orders+.pdf%22&blobheadervalue2=application%2Fpdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1251750315628&ssbinary=true>

Governor's Energy Office. *The Governor's Energy Office Sustainability Policy*. 2008.

<http://rechargecolorado.org/images/uploads/pdfs/GEOenvironmentalpolicy.pdf>

HB 10-1328, CRS 32-20-101, “Concerning The “New Energy Jobs Creation Act Of 2010”, And, In Connection Therewith, Creating The Colorado New Energy Improvement District And Authorizing The District To Fund New Energy Improvements By Issuing Special Assessment Bonds Payable From Special Assessments Levied On Eligible Real Property Owned By Persons Who Voluntarily Join The District In Order To Have The District Help Them Fund New Energy Improvements To The Eligible Real Property.” (2010).

http://www.state.co.us/gov_dir/leg_dir/olls/sl2010a/sl_426.htm

HB 10-1342, CRS 40-2-127, “Concerning Measures to Encourage Additional Investment in Solar Energy Generation Facilities, and, in connection therewith, authorizing the Creation of Community Solar Gardens.” (2010)

<http://www.leg.state.nv.us/Session/76th2011/Exhibits/Assembly/CMC/ACMC665E.pdf>

HB 1281 “An Act Concerning Increased Renewable Energy Standards “(2004)

http://www.ucsusa.org/assets/documents/clean_energy/colorado.pdf

HB 1365, CRS 40-3.2-201, “Clean Air, Clean Jobs Act” (2010)

http://www.state.co.us/gov_dir/leg_dir/olls/sl2010a/sl_140.htm;

http://www.leg.state.co.us/clics/clics2010a/csl.nsf/fsbillcont/47C157B801F26204872576AA00697A3F?Open&file=1001_rer.pdf

SB 07-091, CRS 40-4-116, “An Act Concerning Renewable Resource Generation, Development Areas, and, in Connection Therewith, Creating a Task force, and Making an Appropriation therefor.” (2007)

http://www.state.co.us/gov_dir/leg_dir/olls/sl2007a/sl_316.htm

SB 07-100, CRS 40-2-126, “Establishes Transmission Incentives to Energy Resource Zone.” (2007) <http://www.energyincolorado.org/lpdb/policies/110>

SB 09-297, CRS 40-2-124, “Amendment 37, The Renewable Energy Standard” (2009)

<http://www.dora.state.co.us/puc/rulemaking/Amendment37/Amend37RelatedStatutes.htm>

SB 10-174, CRS 37-90.5-102, “Geothermal Resources Act.” (2010)

<http://ssl.csg.org/dockets/2012cycle/2012volume/2012volumeoriginalbills/0332a02coenrgeothermalenergy.pdf>

SB 11-045, CRS 40-4-110: “Concerning a Streamlines Process for Securing Governmental Approval for the Siting of Electric Transmission Facilities, and, in connection therewith, creating a Task Force.” (2011)

http://www.dora.state.co.us/puc/projects/TransmissionSiting/SB11-45/SB11-45_enr.pdf

SB 11-131, CRS 40-4-118, “Creation of the Colorado Smart Grid Task Force.” (2010)

http://www.leg.state.co.us/clics/clics2011a/csl.nsf/fsbillcont3/31B121E4E9C0548987257801006034F8?Open&file=131_01.pdf

State of Colorado. Colorado Legislative Council Staff. *Amendment 37: Fiscal Impact Statement*. Marc Carey, 7 Sept. 2004.

<http://www.colorado.gov/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1251655496974&ssbinary=true>

Book 2: Energy Assurance Action Plan

Sections IV: Energy Assurance Action Plan: All Sections

- “Article IV, Colorado Constitution.” Balletopedia
http://ballotpedia.org/wiki/index.php/Article_IV,_Colorado_Constitution
- “Colorado Procedures for Emergency Management Assistance Compact Requests.” Colorado Division of Emergency Management. <http://www.coemergency.com/2010/05/colorado-procedures-for-emergency.html>
- “National Response Framework, Resource Center.” FEMA.
<http://www.fema.gov/emergency/nrf/> (with links to: Emergency Support Functions Annex, National Incident Management System)
- “NERC Standards.” North American Electric Reliability Corporation.
<http://www.nerc.com/page.php?cid=2> (with links to: *Standards Process Manual, Reliability Standards*)
- “NIMS Resource Center.” *National Incident Management System*. FEMA
<https://www.fema.gov/emergency/nims/>
- “Resources and Publications.” Colorado Department of Local Affairs
<http://www.colorado.gov/cs/Satellite/DOLA-Main/CBON/1251596812287> (with links to: Elected Official's Policy Guide for Disasters and Emergencies, Colorado Disaster Act- Senate Bill 92-36, Robert T. Stafford Disaster Relief and Emergency Assistance Act, and Intergovernmental Agreement for Emergency Management)

Book 3: Energy Assurance Risk and Vulnerability Assessment

Section IX Risk and Vulnerability Assessment

Assessing Existing Publications, Planning Mechanisms, Reports, and Studies

(Most of the existing publications, planning mechanisms, reports, and studies are cited and accessible directly within the CEAP document.)

Batson, Joni, and R.W. Beck. “Case Study: Potential Value of Distributed Solar Technologies.” Electric Light & Power, POWERGRID International, and Utility Products
<http://www.elp.com/index/display/article-display/1340694064/articles/electric-light-power/volume-88/issue-5/sections/renewables/case-study-potential-value-of-distributed-solar-technologies.html>

Greenhouse Gas Reporting Program. Environmental Protection Agency, 5 June 2012.
<http://www.epa.gov/climatechange/emissions/ghgrulemaking.html>

IPCC- Reports. Intergovernmental Panel on Climate Change
http://www.ipcc.ch/publications_and_data/publications_and_data_reports.shtml

Prevention of Significant Deterioration (PSD) Basic Information. Environmental Protection Agency. <http://www.epa.gov/nsr/psd.html>

Energy Sector Profile

US and Colorado Electric Power System

“Energy Production and Consumption Estimates in Trillion Btu, 2009 (Table).” US Energy Information Association, 2009. http://www.eia.gov/state/seds/sep_prod/pdf/P3.pdf

“Operations and Resource Information: Public Power in Colorado.” Colorado Association of Municipal Utilities. <http://coloradopublicpower.org/Public-Power-in-Colorado/operations-and-resource-information.html>

“Public Law 110 - 343 - Emergency Economic Stabilization Act of 2008.” U.S. Government Printing Office, 3 Oct. 2008. <http://www.gpo.gov/fdsys/pkg/PLAW-110publ343/content-detail.html>

Snider, Laura. “Boulder Municipalization Fact-checking: A Look at Colorado's Municipal Utilities.” Boulder Daily Camera, 18 Oct. 2011.
http://www.dailycamera.com/ci_19121381

“Western Interconnection Balancing Authorities (Map).” Western Electricity Coordinating Council.
<http://www.wecc.biz/library/WECC%20Documents/Publications/Balancing%20Authorities.pdf>

Colorado Energy Resource Profile

Natural Gas

Colorado: Data. U.S. Energy Information Administration.

<http://www.eia.gov/state/state-energy-profiles-data.cfm?sid=CO#Reserves>

Colorado: Overview. U.S. Energy Information Administration. October 2009.

<http://www.eia.gov/state/state-energy-profiles.cfm?sid=CO>

Foss, Michelle M. December 2004. *Interstate Natural Gas—Quality Specifications & Interchangeability.* Center for Energy Economics.

http://www.beg.utexas.edu/energyecon/Ing/documents/CEE_Interstate_Natural_Gas_Quality_Specifications_and_Interchangeability.pdf

Natural Gas: About U.S. Natural Gas Pipelines. Intrastate Natural Gas Pipeline Segment. U.S. Energy Information Administration.

http://www.eia.gov/pub/oil_gas/natural_gas/analysis_publications/ngpipeline/intrastate.html

Natural Gas: About U.S. Natural Gas Pipelines. Natural Gas Pipelines in the Central Region. Energy Information Administration.

http://www.eia.gov/pub/oil_gas/natural_gas/analysis_publications/ngpipeline/central.html

Natural Gas: About U.S. Natural Gas Pipelines. Transportation Process and Flow. U.S. Energy Information Administration.

http://www.eia.gov/pub/oil_gas/natural_gas/analysis_publications/ngpipeline/process.html

Pipeline Safety Community. PHMSA. U.S. Department of Transportation Pipeline and Hazardous Materials Administration. <http://phmsa.dot.gov/pipeline>

Tobin, James. December 3, 2003. *Natural Gas Market Centers and Hubs: A 2003 Update.* U.S. Energy Information Administration.

http://www.eia.gov/pub/oil_gas/natural_gas/feature_articles/2003/market_hubs/mkthubs_web.html

Renewable Resources

2010 Colorado Utilities Report. Colorado Governor's Energy Office, 2010.

http://rechargecolorado.org/images/uploads/pdfs/2010_Colorado_Utilities_Report_7-26-10.pdf

“Biodiesel Monthly Report,” US Energy Information Administration. October 2010

<http://205.254.135.7/totalenergy/data/annual/showtext.cfm?t=ptb1004>

“Biofuels in the U.S. Transportation Sector.” US Energy Information Administration. February 2007 <http://www.eia.gov/oiaf/analysispaper/biomass.html>

Chambers, Nicholas. “Storing the Sun.” The Crestone Eagle Newspaper, Mar. 2009. http://www.crestoneagle.com/archives2009/mar09_b1.html

“Colorado 6th for Wind Energy's Share of Power,” *Denver Business Journal*, April 12, 2012 <http://www.bizjournals.com/denver/news/2012/04/12/colorado-6th-for-wind-energys-share.html>

Colorado: Overview. U.S. Energy Information Administration. October 2009. <http://www.eia.gov/state/state-energy-profiles.cfm?sid=CO>

“Colorado Study Finds More Geothermal Energy.” *Reuters*, 8 Feb 2007 <http://www.reuters.com/article/2007/02/08/colorado-geothermal-idUSN0842341020070208>

“Geothermal Energy Fact Sheet,” Colorado Renewable Energy Society, March 2011 <http://www.geo-energy.org/Resources.aspx>

Gordon, Nicole. “A Whirlwind of Research: NCAR Delves Into Wind-Energy Prediction and Impacts.” University Corporation for Atmospheric Research Quarterly, Winter 2008-2009. <http://www.ucar.edu/communications/staffnotes/09pdfs/JanFeb09.pdf>

“How Much of Our Energy is Generated from Renewable Sources?” Energy in Brief, Energy Information Administration, Sep 2010 http://205.254.135.7/energy_in_brief/renewable_electricity.cfm

Joel Makower, Ron Pernick, and Clint Wilder. *Clean Energy Trends*. Clean Edge, 2009 <http://cleanedge.com/reports/clean-energy-trends-2012>

“Renewables in global energy supply: An IEA facts sheet.” International Energy Agency, 2007 http://www.iea.org/papers/2006/renewable_factsheet.pdf

Coal

2010 Colorado Utilities Report. Colorado Governor's Energy Office, 2010. http://rechargecolorado.org/images/uploads/pdfs/2010_Colorado_Utilities_Report_7-26-10.pdf

“2010 Summary Statistics (Table).” U.S. Energy Information Association. http://www.eia.gov/state/seds/sep_prod/pdf/P3.pdf

“Annual Coal Distribution Report.” *Coal: Analysis and Predictions*. U.S. Energy Information Administration, 30 Nov. 2011. <http://www.eia.gov/coal/distribution/annual/>

“Energy Resources-Coal.” Colorado Geological Survey, 18 Mar. 2012. <http://geosurvey.state.co.us/energy/Coal/Pages/Coal.aspx>

- “Mining Methods” Colorado Geological Survey, 31, May 2011.
<http://geosurvey.state.co.us/energy/Coal/MiningMethods/Pages/Methods.aspx>
- “Mining Statistics.” *NIOSH Office of Mine Safety and Health Research*. Centers for Disease Control and Prevention, 30 Mar. 2012.
<http://www.cdc.gov/niosh/mining/statistics/>
- “U.S. Coal Supply and Demand: 2010 Year in Review.” U.S. Energy Information Administration, 1 June 2011 http://www.eia.gov/coal/review/coal_prices.cfm
- “Xcel Energy Files 2011 Resource Plan for Energy Needs through 2018.” *News Archive*. Xcel Energy, 31 Oct. 2011.
http://www.xcelenergy.com/About_Us/Energy_News/News_Archive/Xcel_Energy_files_2011_resource_plan_for_energy_needs_through_2018
- Hydroelectric**
- Bosner, Kevin. “Hydropower Plants.” HowStuffWorks,
<http://science.howstuffworks.com/environmental/energy/hydropower-plant1.htm>
- Chambers, Nicholas. “Storing the Sun.” *The Crestone Eagle Newspaper*, Mar. 2009.
http://www.crestoneagle.com/archives2009/mar09_b1.html
- Connecting Colorado's Renewable Resources to the Markets: Report of the Colorado Senate Bill 07-091 Renewable Resource Generation Development Areas Task Force. Colorado Governor's Energy Office, 2007.
<http://www.colorado.gov/cs/Satellite?blobcol=urldata&blobheadername1=Content-Disposition&blobheadername2=Content-Type&blobheadervalue1=inline%3B+filename%3D%22REDI+Report+%28Full+Version%29.pdf%22&blobheadervalue2=application%2Fpdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1251746588129&ssbinary=true>
- “Hydroelectric.” *Renewable and Alternative Fuels*. US Energy Information Administration
<http://www.eia.gov/cneaf/solar.renewables/page/hydroelec/hydroelec.html>
- “Hydroelectric Power Water Use.” US Geological Survey, 9 Mar. 2012.
<http://ga.water.usgs.gov/edu/wuhy.html>
- ”Hydroelectricity.” Environmental Protection Agency, 28 Dec. 2007.
<http://www.epa.gov/cleanenergy/energy-and-you/affect/hydro.html>
- “Identify Drought Vulnerable Sectors in Colorado” www.drought.unl.edu/portals/0/docs/CO_drought_vulnerable_sectors.doc
- “Pumped Storage.” *Power Partners Resource Guide*. Power Partners.
<http://www.uspowerpartners.org/Topics/SECTION2Topic-PumpedStorage.htm>

Liquid Fuels

Colorado: Overview. U.S. Energy Information Administration. October 2009.

<http://www.eia.gov/state/state-energy-profiles.cfm?sid=CO>

“Domestic Supply of Liquid Fuels Projected to Increase, Resulting in Fewer Imports.” US Energy Information Administration, 26 Jan. 2012.

<http://www.eia.gov/todayinenergy/detail.cfm?id=4730>

Liquid Fuels Emergency Action Plan: ESF12b Energy. Colorado Governor's Energy Office, 2009.

“Primary US Energy Consumption: Liquid Fuel Is the Largest Source of Energy Consumption in America.” Sapphire Energy. <http://www.sapphireenergy.com/learn-more/59456-primary-us-energy-consumption-liquid-fuel>

Smart Grid and Distributed Generation

Doran, Kevin, Frank Barnes, and Puneet Pasrich. “Smart Grid Deployment in Colorado: Challenges and Opportunities.” University of Colorado at Boulder, June 2010.

<http://cees.colorado.edu/sgreport.pdf>

Costs and Strategic Approaches to Disruption

David Lineweber and Shawn McNulty. “The Cost of Power Disturbances to Industrial & Digital Economy Companies,” Consortium for Electric Infrastructure to Support Digital Society (CEIDS), Electric Power Research Institute (EPRI), June 2001

http://intelligrid.epri.com/docs/Cost_of_Power_Disturbances_to_Industrial_and_Digital_Technology_Companies.pdf

Joseph Seymour and Terry Horsley. “The Seven Types of Power Problems.” White Paper #18. American Power Conversion, 2005.

<http://www.hvacovervoltage.com/info/PowerProblems.pdf>

Kristina Hamachi-LaCommare and Joseph H. Eto. “Understanding the Cost of Power Interruptions to U.S. Electricity Consumers.” Ernest Orlando Lawrence Berkeley National Laboratory. Environmental Energy Technologies Division, September 2004.

<http://certs.lbl.gov/pdf/55718.pdf>

Sylves, Richard. Disaster Policy & Politics: Emergency Management and Homeland Security. Congressional Quarterly (CQ) Press, 2008

Energy Sector Interdependencies

Interdependencies and Systemic Failures

Gaspard, Francois, and Alain Hubrecht. “Tackling Critical Energy Infrastructure Network Interdependencies.” Journal of Energy Security, 23 Mar. 2010.

http://www.ensec.org/index.php?option=com_content

James P. Peerenboom, Ronald E. Fisher, “Analyzing Cross-Sector Interdependencies,” *hicss*, pp.112a, 40th Annual Hawaii International Conference on System Sciences (HICSS'07), 2007 <http://www.computer.org/csdl/proceedings/hicss/2007/2755/00/27550112a-abs.html>

Institute of Public Utilities. *Technical Assistance Briefs: Utility and Network Interdependencies: What State Regulators Need to Know*. National Association of Regulatory Utility Commissioners, 2005. http://www.naruc.org/Publications/CIP_Interdependencies_2.pdf

Energy Infrastructure Interdependency Failures: Case Studies

“3 Nuclear Reactors melted down after Quake, Japan Confirms.” CNN, 07 June 2011. <http://edition.cnn.com/2011/WORLD/asiapcf/06/06/japan.nuclear.meltdown/index.html?ref=NS1>

“Analysis: A Month On, Japan Nuclear Crisis Still Scarring.” International Business Times, 08 Apr. 2011. <http://in.ibtimes.com/articles/132391/20110409/japan-nuclear-crisis-radiation.htm>

Associated Press. “Texas Senate To Investigate Rolling Blackouts.” CBS Dallas Ft. Worth, 15 Feb. 2011. <http://dfw.cbslocal.com/2011/02/15/texas-senate-to-investigate-rolling-blackouts>

Baltimore, Chris. “Texas Weathers Rolling Blackouts as Mercury Drops.” *Reuters*. Thomson Reuters, 02 Feb. 2011. <http://www.reuters.com/article/2011/02/02/us-ercot-rollingblackouts-idUSTRE7116ZH20110202>

Barton, Charles. “Texas Power Blackouts and Green Energy.” The Energy Collective, 4 Feb. 2011. <http://theenergycollective.com/charlesbarton/51063/tesas-power-blackouts-and-green-energy>

“ERCOT Announces End to Rolling Blackouts.” American Statesman, 2 Feb. 2011. http://www.statesman.com/blogs/content/shared-gen/blogs/austin/weather/entries/2011/02/02/statewide_power.html

Fehling, Dave. “Keeping the Lights On in Texas.” KUT.org, 22 May 2012. <http://kut.org/2012/05/keeping-the-lights-on-in-texas/>

“Fukushima Nuclear Accident Update Log.” IAEA. <http://www.iaea.org/newscenter/news/2011/fukushima150311.html>

Helman, Christopher. “Rolling Blackouts Force Texas To Import Power From Mexico.” *Forbes Magazine*, 03 Feb. 2011. <http://www.forbes.com/sites/christopherhelman/2011/02/03/rolling-blackouts-force-texas-to-import-power-from-mexico/>

Miller, Charles, Amy Cabbage, Daniel Dorman, Jack Grobe, Gary Holahan, and Nathan Sanfilippo. *Recommendations for Enhancing Reactor Safety In the 21st Century: The Near-Term Task Force Review of Insights from the Fukushima Dai-ichi Accident*. US

Nuclear Regulatory Commission, 2011.
<http://pbadupws.nrc.gov/docs/ML1118/ML111861807.pdf>

“New USGS Number Puts Japan Quake at 4th Largest.” CBS News, 14 Mar. 2011.
<http://www.cbsnews.com/stories/2011/03/14/501364/main20043126.shtml>

Souder, Elizabeth, S.C Gwynne, and Gary Jacobson. “Freeze Knocked out Coal Plants and Natural Gas Supplies, Leading to Blackouts.” The Dallas Morning News, 6 Feb. 2011.
<http://www.dallasnews.com/news/state/headlines/20110206-freeze-knocked-out-coal-plants-and-natural-gas-supplies-leading-to-blackouts.ece>

Stevens, Andrew. “After Fukushima: Japan's Energy Crisis.” *Business 360*. CNN, 9 Sept. 2011.
<http://business.blogs.cnn.com/2011/09/09/after-fukushima-japans-energy-crisis/>

Strickland, Eliza. “What Went Wrong in Japan's Nuclear Reactors.” IEEE Spectrum, 16 Mar. 2011. <http://spectrum.ieee.org/tech-talk/energy/nuclear/explainer-what-went-wrong-in-japans-nuclear-reactors>

Tabuchi, Hiroko, and Keith Bradsher. “Japan Says 2nd Reactor May Have Ruptured with Radioactive Release.” The New York Times, 15 Mar. 2011.
http://www.nytimes.com/2011/03/16/world/asia/16nuclear.htm?_r=2

Ube, Mitsuru. “Tepco President Says State Could Take Stake in Firm.” *Business*. Wall Street Journal, 14 Dec. 2011.
<http://online.wsj.com/article/SB10001424052970204026804577097652917740774.html>

High Impact/Low Probability Events

High-Impact, Low-Frequency Event Risk to the North American Bulk Power System: A Jointly-Commissioned Summary Report of the North American Electric Reliability Corporation and the U.S. Department of Energy’s November 2009 Workshop. 2010.
<http://www.nerc.com/files/HILF.pdf>

Cyber Warfare

Assante, Michael. “Critical Cyber Asset Identification.” Letter to Industry Stakeholders. 7 Apr. 2009. North American Electric Reliability Corporation
<http://online.wsj.com/public/resources/documents/CIP-002-Identification-Letter-040609.pdf>

Clarke, Richard. “China's Cyberassault on America.” *Opinion*. Wall Street Journal, 15 June 2011.
http://online.wsj.com/article/SB10001424052702304259304576373391101828876.html?mod=WSJ_hp_mostpop_read

Clarke, Richard. *Cyber War*. N.p.: Harper Collins, 2010.

- “Computer Security.” *Report Archive*. Guardsmark
http://www.guardsmark.com/library/computer_security.asp?nav=4&subnav=1
- Edwards, David, and Ryan Brynaert. “Disconnect Electrical Grid from Internet, Former Terror Czar Clarke Warns.” *The Raw Story*, 8 Apr. 2009.
http://rawstory.com/news/2008/Richard_Clarke_Disconnect_electrical_grid_from_0408.html
- Gjelten, Tom. “Cyberwarrior Shortage Threatens U.S. Security.” NPR, 19 July 2010.
<http://www.npr.org/templates/story/story.php?storyId=128574055>
- Gorman, Siobahn. “Electricity Grid in U.S. Penetrated By Spies.” *Technology*. Wall Street Journal, 8 Apr. 2009. <http://online.wsj.com/article/SB123914805204099085.html>
- “Hackers Reportedly Have Embedded Code in Power Grid.” (Video) CNN, 9 Apr. 2009.
<http://www.cnn.com/2009/TECH/04/08/grid.threat/index.html?iref=newssearch>
- Holland, Steve, and Randall Mikkelson. “UPDATE 2-US Concerned Power Grid Vulnerable to Cyber-attack.” *Rueters*, 08 Apr. 2009.
<http://in.reuters.com/article/2009/04/08/cyberattack-usa-idINN0853911920090408>
- Lynne III., William J. “Defending a New Domain: The Pentagon's Cyberstrategy.” *Foreign Affairs*, Sept.-Oct. 2010. <http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain>
- “Power Grid Penetrated?” *Fox News*, 1 May 2011. <http://video.foxnews.com/v/3927859/>
- Shiels, Maggie. “Spies 'infiltrate US Power Grid’” *BBC*, 04 Sept. 2009.
<http://news.bbc.co.uk/2/hi/technology/7990997.stm>
- “Spies Penetrate U.S. Power Grid: Report Says Russian and Chinese Operatives Could Disrupt Electric System.” *ABC News Video*. ABC News.
<http://abcnews.go.com/Video/playerIndex?id=7286823>
- Tong, Xiong. “China Denies Intruding into U.S. Electrical Grid_English_Xinhua.” *Window of China*. China View, 9 Apr. 2009. http://news.xinhuanet.com/english/2009-04/09/content_11157765.htm
- “The Threat from the Internet: Cyberwar.” *The Economist Newspaper*, 01 July 2010.
http://www.economist.com/node/16481504?story_id=16481504
- Xiaohuo, Cui. “‘China Threat’ Theory Rejected.” *China Daily*, 9 Apr. 2009.
http://www.chinadaily.com.cn/china/2009-04/09/content_7661885.htm

Solar Weather

- Kappenman, John. “Geomagnetic Storms and Their Impacts on the U.S. Power Grid.” Oakridge National Laboratory, Jan. 2010. http://www.ornl.gov/sci/ees/etsd/pes/ferc_emp_gic.shtml

Phillips, Tony. "Severe Space Weather--Social and Economic Impacts." NASA, 21 Jan. 2009.
http://science.nasa.gov/science-news/science-at-nasa/2009/21jan_severespaceweather

SpaceWeather.com. <http://www.spaceweather.com/>

NWS Space Weather Prediction Center. NOAA. <http://www.swpc.noaa.gov/>

Book 3A: Hazard Typology and Quick Reference Guide™

Section X: Hazard Typology and Quick Reference Guide™

Hazard Quick Reference Guide

Drought

Colorado Division of Emergency Management. “Section 3: Hazard Identification and Risk Assessment.” *State of Colorado Natural Hazards Mitigation Plan*. January 2011
<http://www.colorado.gov/cs/Satellite/DOLA-Main/CBON/1251595686517>

Colorado Water Conservation Board. *Drought and Water Supply Assessment*. 2004.
<http://cwcb.state.co.us/technical-resources/colorado-drought-water-supply-assessment/Pages/main.aspx>

“Drought Incident: Incident Annex X.” *Colorado State Emergency Operations Plan*. Division of Emergency Management, 2010. www.colorado.gov/cs/Satellite/DOLA-Main/CBON/1251595696267

“Drought Monitor Archives.” *Drought Impact Reporter*. National Drought Mitigation Center.
<http://droughtmonitor.unl.edu/archive.html>

McKee, Thomas B., Nolan J. Doesken, John Kleist, Colorado Climate Center, Colorado State University Atmospheric Science Department, Catherine J. Shrier, and William P. Stanton. *A History of Drought in Colorado: Lessons Learned and What Lies Ahead*. 2nd ed. No. 9. February 2000. <http://ccc.atmos.colostate.edu/pdfs/ahistoryofdrought.pdf>

Flood

“30 Years after Deadly Big Thompson Flood.” *Big Thompson Flood: July 31, 1976*. Reporter-Herald, 2006. <http://www.colorado.com/reporterherald/1976flood/index.asp>

Colorado Division of Emergency Management. “Section 3: Hazard Identification and Risk Assessment.” *State of Colorado Natural Hazards Mitigation Plan*. January 2011.
<http://www.colorado.gov/cs/Satellite/DOLA-Main/CBON/1251595686517>

Flood Hazard Mitigation Plan for Colorado. August 2007.

“Flood Incident: Incident Annex VI.” *Colorado State Emergency Operations Plan*. Division of Emergency Management, 2010. www.colorado.gov/cs/Satellite/DOLA-Main/CBON/1251595696267

“Flood Summary July 31- Aug. 1, 1976.” *The Weather and Climate Impact Assessment Science Initiative*. University Corporation for Atmospheric Research (UCAR).
http://www.assessment.ucar.edu/flood/flood_summaries/07_31_1976.html

“Flood Water Exposure.” *Water Related Emergencies and Outbreaks*. Centers for Disease Control and Prevention, 25 Aug. 2010.

<http://www.cdc.gov/healthywater/emergency/flood/index.html>

“Most Damaging Floods in Colorado.” *The Weather and Climate Impact Assessment Science Initiative*. University Corporation for Atmospheric Research

http://www.assessment.ucar.edu/flood/flood_table.html

Reidell, Tony. “Historical Colorado Flood Events.” *Colorado Division of Emergency Management*. Colorado Department of Local Affairs, 20 Jan. 2010.

<http://www.coemergency.com/2010/01/historical-colorado-flood-events.html>

Lightning

Colorado Division of Emergency Management. “Section 3: Hazard Identification and Risk Assessment.” *State of Colorado Natural Hazards Mitigation Plan*. January 2011.

<http://www.colorado.gov/cs/Satellite/DOLA-Main/CBON/1251595686517>

Hodanish, Stephen, and Paul Wolyn. *Lightning Climatology for the State of Colorado*. NOAA/NWS Pueblo, Colorado.

www.crh.noaa.gov/Image/pub/lgt2/CO_lgt_climo_5sep.pdf

“Lightning Flash Density Map of Colorado: County Outlines Only.” *National Weather Service Pueblo Lightning Page*.

http://www.crh.noaa.gov/pub/?n=/lgt/flash_density_maps_index.php

Tornadoes

Colorado Division of Emergency Management. “Section 3: Hazard Identification and Risk Assessment.” *State of Colorado Natural Hazards Mitigation Plan*. January 2011.

<http://www.colorado.gov/cs/Satellite/DOLA-Main/CBON/1251595686517>

Hake, Tony. “Windsor Marks One Year Anniversary of EF3 Tornado.” *Examiner*.

<http://www.examiner.com/weather-in-denver/windsor-marks-one-year-anniversary-of-ef3-tornado>

McGhee, Tom. “One Year Later in Windsor.” *The Denver Post*, 22 May 2009.

http://www.denverpost.com/breakingnews/ci_12424988?source=pkg

“Mile-wide Tornado Hits Windsor, Weld County.” *The Denver Post*, 22 May 2008.

http://www.denverpost.com/breakingnews/ci_9344925

“Storm Prediction Center Severe Weather GIS (SVRGIS) Page.” *Storm Prediction Center*. NOAA's National Weather Service, 2011.

<http://www.spc.ncep.noaa.gov/gis/svrgis/>

“U.S. Tornado Climatology.” *Tornado Climatology*. NOAA Satellite and Information Service: National Climatic Data Center, 2012.

<http://www.ncdc.noaa.gov/oa/climate/severeweather/tornadoes.html>

Wind

Colorado Division of Emergency Management. “Section 3: Hazard Identification and Risk Assessment.” *State of Colorado Natural Hazards Mitigation Plan*. January 2011. <http://www.colorado.gov/cs/Satellite/DOLA-Main/CBON/1251595686517>

“State of the Climate National Overview.” NOAA Satellite and Information Service; National Climatic Data Center, Feb. 2012. <http://www.ncdc.noaa.gov/sotc/national/>

“Storm Prediction Center Severe Weather GIS (SVRGIS) Page.” *Storm Prediction Center*. NOAA's National Weather Service, 2011. <http://www.spc.ncep.noaa.gov/gis/svrgis/>

Wind Zones in the United States.” FEMA, 11 Aug. 2010. http://www.fema.gov/plan/prevent/saferoom/tsfs02_wind_zones.shtm

Avalanche

Berwyn, Bob. “Colorado Experts Warn of Dangerous Snow and Mudslides.” Summit County Citizens Voice. <http://summitcountyvoice.com/2011/05/06/colorado-experts-warn-of-dangerous-snow-and-mudslides/>

“CAIC: Colorado Avalanche Information Center.” <http://avalanche.state.co.us/index.php>

Colorado Division of Emergency Management. “Section 3: Hazard Identification and Risk Assessment.” *State of Colorado Natural Hazards Mitigation Plan*. January 2011. <http://www.colorado.gov/cs/Satellite/DOLA-Main/CBON/1251595686517>

Wildfire

Colorado Division of Emergency Management. “Section 3: Hazard Identification and Risk Assessment.” *State of Colorado Natural Hazards Mitigation Plan*. January 2011. <http://www.colorado.gov/cs/Satellite/DOLA-Main/CBON/1251595686517>

Fourmile Canyon Fire Assessment Team. *Fourmile Canyon Fire Preliminary Findings*. Rep. US Dept of Agriculture Forest Service, 2011. <http://www.fs.fed.us/rmrs/docs/fourmile-canyon-fire/preliminary-findings.pdf>

Gabbert, Bill. “NICC Releases Wildfire Stats for 2010.” *Wildfire Today*. <http://wildfiretoday.com/2011/02/10/nicc-releases-wildfire-stats-for-2010/>

Hayman Fire Case Study: Summary. USDA Forest Service. http://www.fs.fed.us/rm/pubs/rmrs_gtr114/rmrs_gtr114_001_032.pdf

“Ongoing Coverage: Fourmile Canyon Fire.” Daily Camera. <http://www.dailycamera.com/fourmile-canyon-fire/>

Extreme Heat

Colorado Division of Emergency Management. "Section 3: Hazard Identification and Risk Assessment." *State of Colorado Natural Hazards Mitigation Plan*. January 2011. <http://www.colorado.gov/cs/Satellite/DOLA-Main/CBON/1251595686517>

Meehl, Gerald A., and Claudia Tebaldi. "More Intense, More Frequent, and Longer Lasting Heat Waves in the 21st Century." *Science* 305.5686 (2004): 994-97. <http://www.sciencemag.org/content/305/5686/994.full>

Hail

Colorado Division of Emergency Management. "Section 3: Hazard Identification and Risk Assessment." *State of Colorado Natural Hazards Mitigation Plan*. January 2011. <http://www.colorado.gov/cs/Satellite/DOLA-Main/CBON/1251595686517>

"Denver Weather History." National Weather Service Denver-Boulder, CO. <http://www.crh.noaa.gov/bou/include/his.php?month=JUL>

"Hail Damage and Statistics." Rocky Mountain Insurance Information Association. 2012. http://www.rmiaa.org/Catastrophes_and_Statistics/Hail.asp

Mitchell, Kirk. "Clean-up Begins after Overnight Metro Denver Storm." *The Denver Post*, 29 July 2009. http://www.denverpost.com/breakingnews/ci_12882385?source=rss

NOAA Severe Weather Primer. NOAA National Severe Storms Laboratory. http://www.nssl.noaa.gov/primer/hail/hail_basics.html

"SPC Preliminary Severe Weather Database Summary." *Storm Prediction Center*. NOAA's National Weather Service, 2011. <http://www.spc.noaa.gov/climo/online/monthly/states.php?month=00>

"SPC Severe Weather Event Review for Monday July 20, 2009." *Storm Prediction Center*. NOAA's National Weather Service. <http://www.spc.noaa.gov/exper/archive/event.php?date=20090720>

Precipitation

Colorado Division of Emergency Management. "Section 3: Hazard Identification and Risk Assessment." *State of Colorado Natural Hazards Mitigation Plan*. January 2011. <http://www.colorado.gov/cs/Satellite/DOLA-Main/CBON/1251595686517>

"Precipitation: Annual Climatology 1971-2000." *Spatial Climate Analysis Service*. 2004. Map.

Thunderstorms

Colorado Division of Emergency Management. "Section 3: Hazard Identification and Risk Assessment." *State of Colorado Natural Hazards Mitigation Plan*. January 2011. <http://www.colorado.gov/cs/Satellite/DOLA-Main/CBON/1251595686517>

“Storm Prediction Center.” NOAA National Weather Service. <http://www.spc.noaa.gov/>

Winter Weather

Colorado Division of Emergency Management. “Section 3: Hazard Identification and Risk Assessment.” *State of Colorado Natural Hazards Mitigation Plan*. January 2011. <http://www.colorado.gov/cs/Satellite/DOLA-Main/CBON/1251595686517>

“March 17-20 2003 Winter Storm.” *Denver March 17-20 2003 Winter Storm*. National Weather Service Weather Forecast Office. http://www.crh.noaa.gov/bou/?n=denstorm_031703

“Winter Storms and Insurance Coverage.” Rocky Mountain Insurance Information Association, 2012. http://www.rmiiia.org/Catastrophes_and_Statistics/Winter_Storms.asp

Earthquake

Colorado Division of Emergency Management. “Section 3: Hazard Identification and Risk Assessment.” *State of Colorado Natural Hazards Mitigation Plan*. January 2011. <http://www.colorado.gov/cs/Satellite/DOLA-Main/CBON/1251595686517>

Colorado Geological Survey Home. <http://geosurvey.state.co.us/Pages/CGSHome.aspx>

“Historic Earthquakes near Denver, Colorado.” *U.S. Geological Survey Earthquake Hazards Program*. USGS. http://earthquake.usgs.gov/earthquakes/states/events/1882_11_08.php

“Quaternary Faults.” *U.S. Geological Survey Earthquake Hazards Program*. <http://earthquake.usgs.gov/hazards/qfaults/co/>

“Quaternary Fault and Fold Database for the United States.” *Denver 1x2 Sheet*. USGS. <http://earthquake.usgs.gov/hazards/qfaults/co/den.html>

Erosion and Deposition

Colorado Division of Emergency Management. “Section 3: Hazard Identification and Risk Assessment.” *State of Colorado Natural Hazards Mitigation Plan*. January 2011. <http://www.colorado.gov/cs/Satellite/DOLA-Main/CBON/1251595686517>

Erosion. Colorado Geological Survey. <http://geosurvey.state.co.us/hazards/Erosion/Pages/Erosion.aspx>

Lane, Anthony. “Mountainous Erosion: Summer Storms Test Drainage Devices along Parts of Pikes Peak Highway.” *Colorado Springs Independent* 30 Aug. 2007. <http://www.csindy.com/colorado/mountainous-erosion/Content?oid=1139601>

Martin, Deborah. *Studies of Post-Fire Erosion in the Colorado Front Range Benefit the Upper South Platte Watershed Protection and Restoration Project*. US Geological Survey. <http://www.watershed.org/?q=node/332>

Moody, John, Deborah A. Martin, and Brian Ebel. "Hydrologic and Erosion Responses of Burned Watersheds." *Geomorphology and Sediment Transport*. USGS, 7 June 2011. http://www.wr.usgs.gov/projects/Burned_Watersheds

"Pikes Peak Watershed Erosion Control and Restoration Project." Rocky Mountain Field Institute. <http://www.rmfi.org/projects/pikes-peak-watershed-erosion-control-and-restoration-project>

Rappold, Scott R. "Paved Road May Help Erosion on Pikes Peak." *Colorado Springs Gazette*, 8 Dec. 2007. <http://www.gazette.com/news/highway-30666-creek-billmeyer.htm>

"Strontia Springs Reservoir Cleanup Nearly Done." *Strontia Springs Reservoir Cleanup Nearly Done*. CBS Denver. CBS4 Denver, 14 July 2011. <http://denver.cbslocal.com/2011/07/14/strontia-springs-reservoir-cleanup-nearly-done/>

Expansive Soils

Colorado Division of Emergency Management. "Section 3: Hazard Identification and Risk Assessment." *State of Colorado Natural Hazards Mitigation Plan*. January 2011. <http://www.colorado.gov/cs/Satellite/DOLA-Main/CBON/1251595686517>

"Expansive Soil and Expansive Clay." Geology.com. <http://geology.com/articles/expansive-soil.shtml>

Swelling Soils. Colorado Geological Survey. <http://geosurvey.state.co.us/hazards/Swelling%20Soils/Pages/SwellingSoils.aspx>

Landslides, Rockslides, and Mudslides

Cannon, Susan H., and Joseph E. Gartner. *Debris-Flow Response of Basins Burned by the 2002 Coal Seam and Missionary Ridge Fires, Colorado*. http://landslides.usgs.gov/docs/cannon/Cannon_etal_AEG_2003.pdf

Colorado Division of Emergency Management. "Section 3: Hazard Identification and Risk Assessment." *State of Colorado Natural Hazards Mitigation Plan*. January 2011. <http://www.colorado.gov/cs/Satellite/DOLA-Main/CBON/1251595686517>

Highland, Lynn M., Ellen D. Stephenson, Sarah B. Christian, and William M. Brown III. "Debris-Flow Hazards in the United States." *U.S. Geological Survey Fact Sheet 176-97*. USGS, 23 June 2003. <http://pubs.usgs.gov/fs/fs-176-97/fs-176-97.html>

Jochim, Candace L., William P. Rogers, John O. Truby, Robert L. Wold Jr, George Weber, and Sally P. Brown. *Colorado Landslide Hazard Mitigation Plan*. 1988. <http://geosurveystore.state.co.us/p-1285-colorado-landslide-hazard-mitigation-plan.aspx>

"Landslide Overview Map of the Conterminous United States." *Landslide Hazards Program*. USGS. <http://landslides.usgs.gov/learning/nationalmap/>

Leib, Jeffery. "Permanent Repairs Begin on Rock-slide-bashed I-70." *The Denver Post*. 23 Mar. 2010. http://www.denverpost.com/ci_14735610?source=pkg

"Post-Wildfire Landslide Hazards" USGS Landslide Hazards Program
<http://landslides.usgs.gov/research/wildfire/>

Subsidence

Colorado Division of Emergency Management. "Section 3: Hazard Identification and Risk Assessment." *State of Colorado Natural Hazards Mitigation Plan*. January 2011.
<http://www.colorado.gov/cs/Satellite/DOLA-Main/CBON/1251595686517>

Subsidence-Mine. Colorado Geological Survey
<http://geosurvey.state.co.us/hazards/SubsidenceMine/Pages/Subsidence.aspx>

Subsidence-Natural. Colorado Geological Survey
<http://geosurvey.state.co.us/hazards/Subsidence-Natural/Pages/CaseHistories.aspx>

"Geologic Mapping along the I-70 Corridor in Western Colorado." *USGS Geology and Environmental Change Science Center*. USGS. <http://esp.cr.usgs.gov/info/i70/index.html>

Human Caused Hazards

Allison, Graham. *Nuclear Terrorism: The Ultimate Preventable Catastrophe*. Holt Paperbacks, 2005.

Almirall, Jose R. "Introduction to Drugs and Explosives Detection." *National Institute of Justice*. Proc. of Technology Transition Workshop.
http://projects.nfstc.org/tech_transition/pspme-ims/presentations/Almirall_Intro_Drugs_Explosives.pdf

Atlas, Randall I. *21st Century Security and CPTED Designing for Critical Infrastructure Protection and Crime Prevention*. CRC Pr I Llc, 2012.

Betts, Richard K. "The Soft Underbelly of American Primacy." *Terrorism and Counterterrorism: Understanding the New Security Environment*. Ed. Russell Howard. McGraw-Hill, 2008.

Clarke, Richard. *Cyber War: The Next Threat to National Security and What to Do About It*. ECCO, 2010.

Claudia Copeland and Betsy Cody. "Terrorism and Security Issues Facing the Water Infrastructure Sector." Congressional Research Service CRS Report for Congress, May 21, 2003

Colorado Division of Emergency Management. "Section 3: Hazard Identification and Risk Assessment." *State of Colorado Natural Hazards Mitigation Plan*. January 2011.
<http://www.colorado.gov/cs/Satellite/DOLA-Main/CBON/1251595686517>

- Couch, Dick, and John Boswell. U.S. Armed Forces Nuclear, Biological And Chemical Survival Manual. Basic, 2003.
- “Council on Foreign Relations.” *Responding to Chemical Attacks*. Council on Foreign Relations, Jan. 2006. <http://www.cfr.org/preparedness/responding-chemical-attacks/p9592>
- Crenshaw, Martha. “The Logic of Terrorism: Terrorist Behavior as a Product of Strategic Choice.” *Terrorism and Counterterrorism: Understanding the New Security Environment*. Ed. Russell Howard. McGraw-Hill, 2008.
- Dishman, Chris. “The Leaderless Nexus: When Crime and Terror Converge.” *Terrorism and Counterterrorism: Understanding the New Security Environment*. Ed. Russell Howard. McGraw-Hill, 2008.
- Fennelly, Lawrence J. *Effective Physical Security*. Boston, Mass: Butterworth-Heinemann, 1997.
- Ferguson, Charles D., Tahseen Kazi, and Judith Birira. *Commercial Radioactive Sources: Surveying the Security Risks*. Monterey, CA: Monterey Institute of International Studies, Center for Nonproliferation Studies, 2003.
- Hoffman, Bruce. *Inside Terrorism*. New York: Columbia UP, 1998.
- Ibanez, McCalley, Aliprantis, Brown, Gkritza, Somani, and Wang. “National Energy and Transportation Systems: Interdependencies within a Long Term Planning Model.” Departments of Electrical and Computer Engineering and Industrial and Manufacturing Systems Engineering. Iowa State University, 2008.
<http://home.eng.iastate.edu/~eibanez/files/Ibanez-NationalEnergyAndTransportationSystems.pdf>
- King, Gilbert. *Dirty Bomb: Weapon of Mass Disruption*. New York, NY: Chamberlain Bros., 2004.
- King, Kevin, Michael Opheim, and Nicholas Bowen. “Redefining US Energy Security in the Twenty First Century.” *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti. CRC, 2008.
- Larsen, Jeffrey and James Wirtz. “WMD Terrorism: New Threats, Revised Responses.” *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti. CRC, 2008.
- Lifton, Robert Jay. *Destroying the World to save it: Aum Shinrikyo, Apocalyptic Violence, and the New Global Terrorism*. New York: Henry Holt and, 1999.
- Mandel, Robert. *Dark Logic: Transnational Criminal Tactics and Global Security*. Stanford, CA: Stanford Security Studies, 2011.
- McKinley, Jesse. “No Cloaks, No Daggers, Just the Mayor.” *New York Times* 24 July 2008.

- Mueller, John E. *Atomic Obsession: Nuclear Alarmism from Hiroshima to Al-Qaeda*. Oxford, 2009.
- . *Illicit: How Smugglers, Traffickers and Copycats Are Hijacking the Global Economy*. New York: Doubleday, 2005.
- North American Electric Reliability Corporation. *Long-Term Reliability Assessment 2009-2018*. 2009. http://www.nerc.com/files/2009_LTRA.pdf
- “The Omega Files: A True Story.” *CNN*. 27 June 2000.
- Pederson, Dudenhoeffer, Hartley, and Permann. “Critical Infrastructure Interdependency Modeling: A Survey of US and International Research.” Idaho National Laboratory, Aug 2006.
- Poulsen, Kevin. “Hacker Disables More Than 100 Cars Remotely.” *Wired* (2010).
- Rid, Thomas. “Think Again: Cyberwar.” *Foreign Policy* (March/April 2012).
- Ring, J. P. “Radiation Risks and Dirty Bombs.” *The Radiation Safety Journal, Health Physics* 86.1 (2004): S42-47.
- Rost, Johann, and Robert L. Glass. *The Dark Side of Software Engineering: The Ethics and Realities of Subversion, Lying, Espionage, and Other Nefarious Activities*. Oxford: Wiley-Blackwell, 2011.
- Shea, Dana A., and Frank Gottron. *Small-scale Terrorist Attacks Using Chemical and Biological Agents an Assessment Framework and Preliminary Comparisons*. [Washington, D.C.]: Congressional Information Service, Library of Congress, 2004.
- Singel, Ryan. “San Francisco Held Cyber-Hostage? Disgruntled Techies Have Wreaked Worse Havoc.” *Wired* (2008).
- Smith, James and Brent Talbot. “Terrorism and Deterrence by Denial.” *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti. CRC, 2008.
- Sylves, Richard. *Disaster Policy & Politics: Emergency Management and Homeland Security*. Washington DC: CQ, 2008.
- Szyliowicz, Joseph. “Transportation as a Component of Homeland Security Strategy.” *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti. CRC, 2008.
- The National Academies and the Department of Homeland Security. *IED Attack: Improvised Explosive Devices Fact Sheet*. National Academies and the Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet.pdf

Wehling, Fred and Jeremy Tamsett. "Nuclear and Radioactive Threats to Homeland Security: New Threats, Revised Responses." *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti. CRC, 2008.