

RELIABILITYFIRST 2023 RECOGNITION AWARDS

Diane Holder, Vice President Entity Engagement and Corporate Services

September 26, 2023





DIANE HOLDER

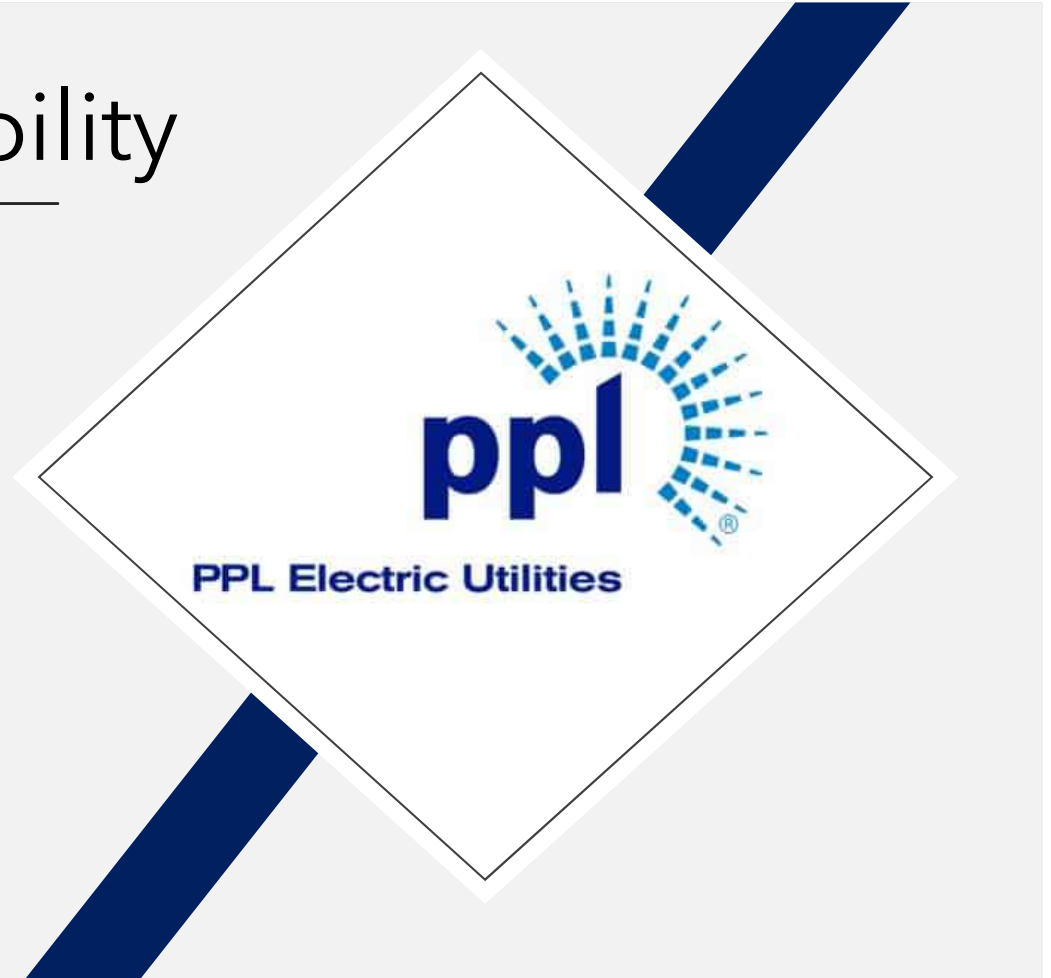
VICE PRESIDENT ENTITY ENGAGEMENT AND
CORPORATE SERVICES, RELIABILITYFIRST

PPL ELECTRIC UTILITIES CORPORATION

Innovation in Reliability

Facility Ratings

- › PPL employs proactive Dynamic Line Ratings (DLR) to ensure the grid is operating efficiently using the data provided by the DLR sensors
- › PPL investigated any CIP requirements that may apply to the sensors and discussed with ReliabilityFirst so that they could proactively address



AES OHIO

Collaboration & Audit Readiness

- › AES Ohio was transparent, collaborative, and timely with initial evidence submissions and throughout the audit process
- › AES Ohio goes beyond the standards by completing quarterly FAC-003 arial inspections and proactively communicating recurring discrepancies to TOs and PCs under PRC-026

The logo for AES Ohio is centered within a white diamond shape. The word "aes" is written in a lowercase, rounded font with a color gradient from blue to green. The word "Ohio" is written in a black, sans-serif font to the right of "aes".

aes Ohio

AES INDIANA

Continuous Improvement in Reliability

- › During engagements, AES Indiana ensured the appropriate SMEs, that were highly knowledgeable, were onsite and demonstrated a strong transparency with responses
- › The improvement areas identified in Indiana were communicated internally to AES Ohio and actions were implemented across the operating companies

The logo for AES Indiana is centered within a white diamond shape. The word "aes" is written in a lowercase, sans-serif font with a color gradient from blue to green. To its right, the word "Indiana" is written in a black, sans-serif font. The diamond is set against a light gray background with two dark blue diagonal stripes.

aes Indiana

ITC HOLDINGS CORP

Achievement of Positive Observations

- › ITC volunteered to pilot the Align tool and capture lessons learned as well as completed one of the first FAC-003 walkdowns
- › ITC concluded their CIP and O&P audit with 9 positive observations
- › ITC supported CIP-014 efforts by creating a video to distribute to local law enforcement as a security reminder



A FORTIS COMPANY

CONGRATULATIONS

PPL Electric Utilities Corporation

AES Ohio

AES Indiana

ITC Holdings Corp



RELIABILITYFIRST 2023 FALL WORKSHOP

SEPTEMBER 26-27, 2023 | PITTSBURGH, PA

WELCOME AND LOGISTICS

- Safety Message
- Webex is not being recorded
- Please submit all questions through SLIDO
- We will provide a survey at the end of Day #2
- Presentation slides are posted on the RF website

Join the
conversation at
Slido.com
#RFWorkshop



WELCOME AND LOGISTICS

- Safety Message
- Webex is not being recorded
- Please submit all questions through SLIDO
- We will provide a survey at the end of Day #2
- Presentation slides are posted on the RF website

Join the
conversation at
Slido.com
#RFWorkshop



slido



What city did you travel from; or where are you joining us from?

ⓘ Start presenting to display the poll results on this slide.

TODAY'S AGENDA

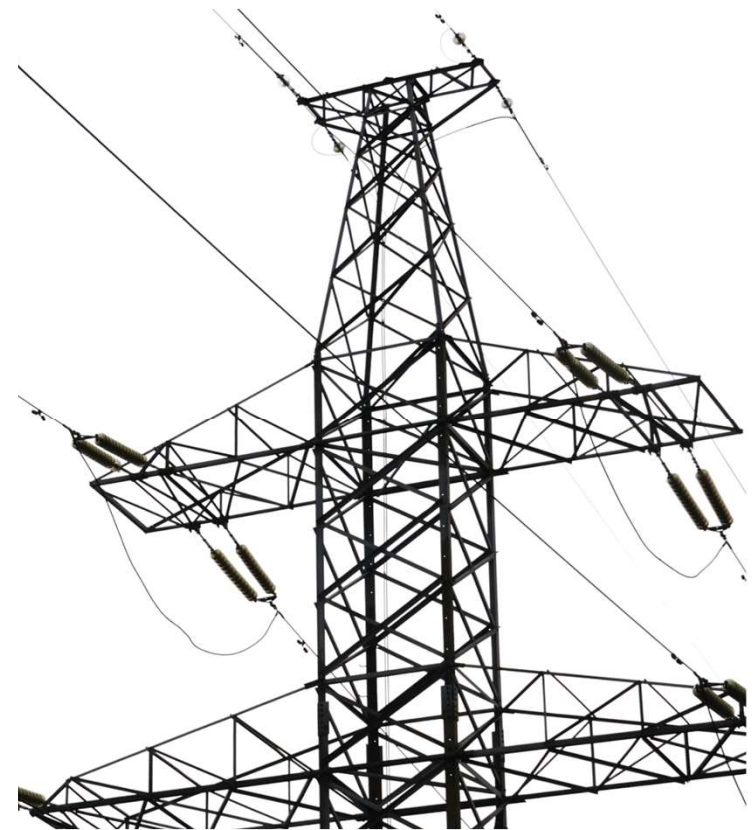
Topic	Speaker(s)
Working Together with State Public Utility Commissions amid the Great Energy Transition	Stephen DeFrank , Chairman, Pennsylvania Public Utility Commission
Human Performance in the Energy Industry	Lesley Evancho , Chief Human Resources Officer, EQT and Independent Director, RF Board of Directors
Securing in Small Bytes: Tactically Addressing Cybersecurity in Critical Infrastructure	Matthew E. Luallen , Lead Research Scientist, Information Trust Institute at the University of Illinois, Urbana-Champaign
Parallels and Interdependencies between the Water and Electric Industries	Justin Ladner , President, Pennsylvania American Water
Panel Discussion: Electric Grid Interdependencies with State Government, Natural Gas, Cybersecurity and Water Industries	Host: Kevin Walker , President and CEO, Duquesne Light Holdings, Inc.



Anti-Trust Statement

It is ReliabilityFirst's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct which violates, or which might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every ReliabilityFirst participant and employee who may in any way affect ReliabilityFirst's compliance with the antitrust laws to carry out this policy.





STEPHEN DEFRANK

CHAIRMAN, PENNSYLVANIA PUBLIC UTILITY
COMMISSION



Stephen M. DeFrank
Chairman, PA Public Utility Commission



- Appointed as Chairman by Gov. Shapiro on August 30, 2023
- Previously served as Vice Chairman since October 27, 2022
- Confirmed as Commissioner by state Senate on October 19, 2022
- Extensive experience in public and private sectors
- Developed utility policy and legislation over 24 years in PA state government
- Member, NARUC Committee on Electricity, NARUC Electric Vehicles State Working Group, NARUC/NASEO Advanced Nuclear State Collaborative, Organization of PJM States (OPSI)

slido



How many bridges are located within the City of Pittsburgh?

ⓘ Start presenting to display the poll results on this slide.

slido



In its most recent Electric Service Reliability Report, the PUC cites this factor as the number one cause for power outages in Pennsylvania:

ⓘ Start presenting to display the poll results on this slide.

slido



As of last summer, approximately how many accounts in Pennsylvania had interconnected net-metered generation?

i Start presenting to display the poll results on this slide.

slido



How many Electric Vehicles are registered in Pennsylvania as of June?

ⓘ Start presenting to display the poll results on this slide.

slido



Currently, there are 27 wind farms in Pennsylvania. What is the total number of megawatts of wind power generation that are installed on Pennsylvania's 27 wind farms?

ⓘ Start presenting to display the poll results on this slide.

slido



This entrepreneur started an electric company in 1886 in Pittsburgh and led the “charge” to assemble and employ the nation’s 1st AC Transformer as well as the first high voltage transmission line in California. Was that entrepreneur....

ⓘ Start presenting to display the poll results on this slide.



Stephen M. DeFrank
Chairman, PA Public Utility Commission



- Appointed as Chairman by Gov. Shapiro on August 30, 2023
- Previously served as Vice Chairman since October 27, 2022
- Confirmed as Commissioner by state Senate on October 19, 2022
- Extensive experience in public and private sectors
- Developed utility policy and legislation over 24 years in PA state government
- Member, NARUC Committee on Electricity, NARUC Electric Vehicles State Working Group, NARUC/NASEO Advanced Nuclear State Collaborative, Organization of PJM States (OPSI)



LESLEY EVANCHO

CHIEF HUMAN RESOURCES OFFICER, EQT

INDEPENDENT DIRECTOR, RF BOARD OF DIRECTORS



Human Performance in the Energy Industry: “It starts with culture”

RF Fall Workshop, September 2023

Introduction

Our Transformation

Culture Strategy

Questions

Who I am: Introduction

Lesley Evancho, CHRO EQT



Focus on Talent Management and Culture

-Led a global Talent-Management function for an industrial safety equipment manufacturer
-Company celebrated it's 100th year during my tenure

🎯 Deep insight into organizational behavior

3

HR Practitioner

-15 Years working in human resources in Western PA
-Manufacturing environments: Union and Non-Union
-High-growth and No-growth environments

🎯 Grew foundation in HR and specifically human capabilities and performance

4

Shifted to Energy Industry

- Joined Rice energy in 2017 as the Head of Human Resources
-Company bought by EQT in the same year

🎯 Understanding of the "economics" of culture

5



CHRO, EQT

-Brought in as part of new Management team, 2019

🎯 Informed, intentional culture aligned with the business

Connect with me:



1

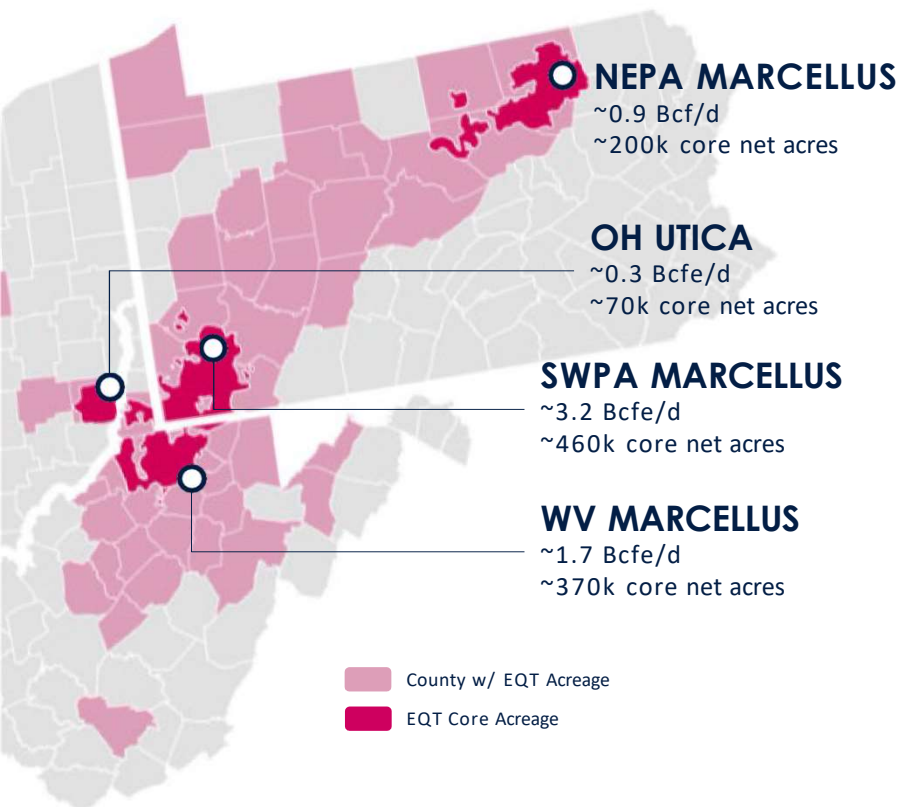
2

Who we are: The Premier North American Natural Gas Producer

Combination of scale, premier assets, and responsible development



PURE-PLAY APPALACHIAN PRODUCER



EQT AT A GLANCE (NYSE: EQT)

<p># 1 Producer of natural gas in the United States⁽⁵⁾</p>	<p>If EQT were a country, it would be the 12th largest producer in the world⁽⁶⁾ (~6% of total US production)</p>	<p>Scale</p>
<p>>1.1 mm Core Acres (Net)</p>	<p>2,100 Core Locations (Net)</p>	
<p>~\$1.8 B Paid to Mineral Owners in 2022</p>	<p>Net Zero By or before 2025⁽⁷⁾ (among the fastest in the industry)</p>	<p>Responsible</p>
<p>Gold-Standard Rating under the OGMP 2.0 Framework (the only comprehensive, measurement-based methane reporting framework for the oil & gas industry)</p>		

1. Share count and share price as of 7/21/2023. 2. Non-GAAP measure. See appendix for definition. Net debt as of 6/30/2023. 3. Long-term (L-T) leverage target assumes \$2.75 natural gas prices. 4. Includes repurchase of senior notes and convertible notes, share buybacks and dividend payments executed through 6/30/2023, including \$29 MM in share repurchases which occurred in December 2021. Inclusive of \$85 MM of principal and \$128 MM of premiums paid for 2026 convertible notes. 5. Source: EIA. 6. Based on Bcf/d production data from S&P Global Commodity Insights as of December 31, 2022. 7. Net zero on a Scope 1 and 2 basis for EQT's Production segment operations and based on assets owned by EQT on 6/30/2021.



RF Fall Workshop

September 2023

Introduction

Our Transformation

Culture Strategy

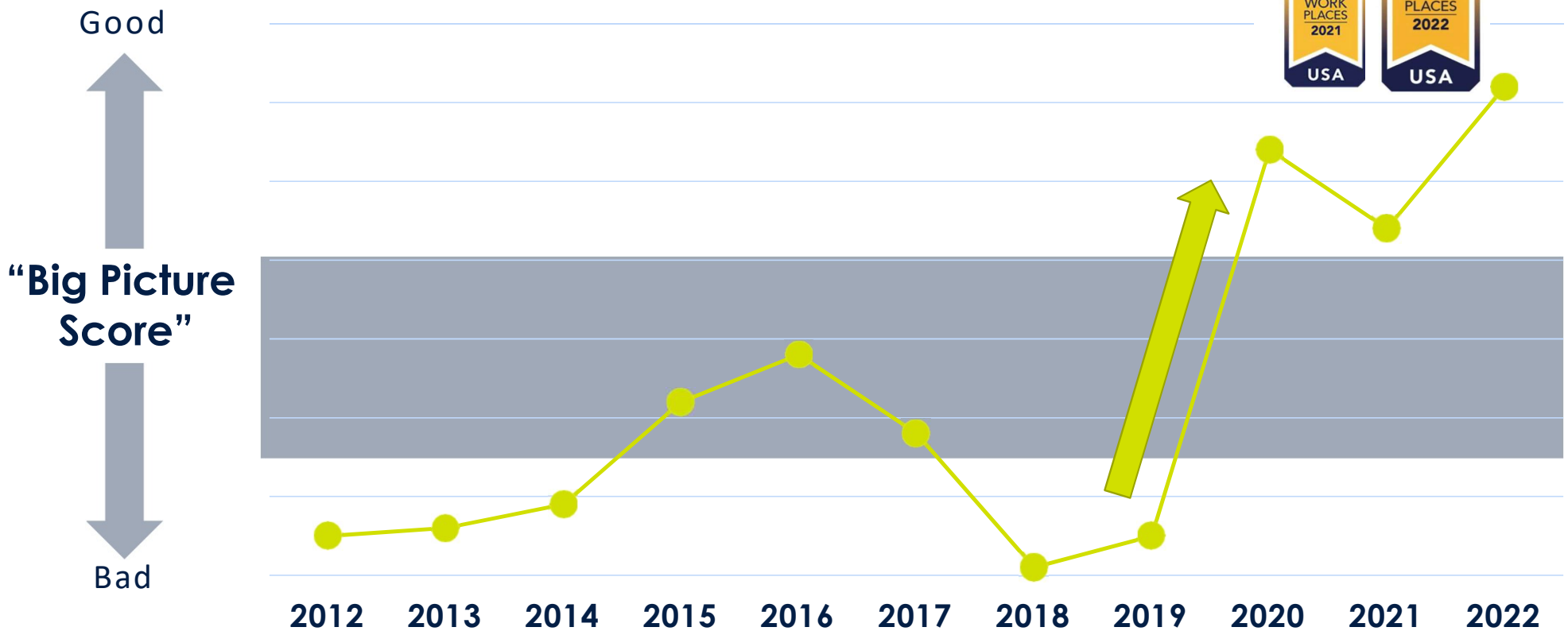
Questions

In less than 1 year, we saw major culture improvement...and it's sustainable

EQT was in the bottom 1/3 percentile, now we are a top workplace



Engagement



Culture: Rapid shift in employee sentiment in less than one year



“These words stood out from our benchmark the most”



Jun 2019



Nov 2020

Green words were used by employees who were more engaged on average.
 Red words were used by employees who were more disengaged on average.
 Highlighted words are your company values.

Culture: Rapid shift in employee sentiment in less than one year



“What 3 words describe the culture at EQT”



Jun 2019



Nov 2020

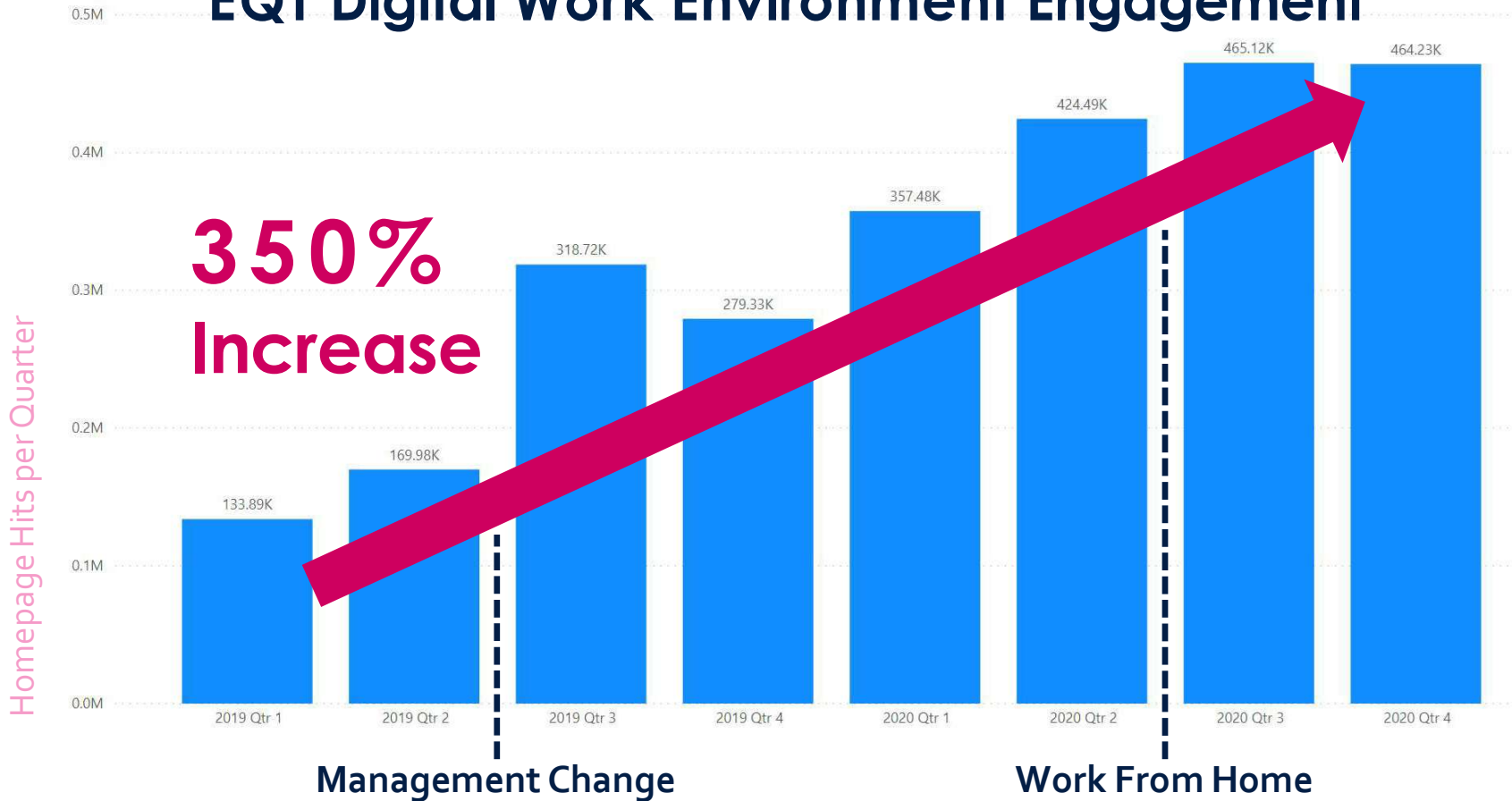
Green words were used by employees who were more engaged on average.
Red words were used by employees who were more disengaged on average.
Highlighted words are your company values.

We jacked up digital engagement...

and powered through the pandemic, enabling transition to a fully remote work from home



EQT Digital Work Environment Engagement

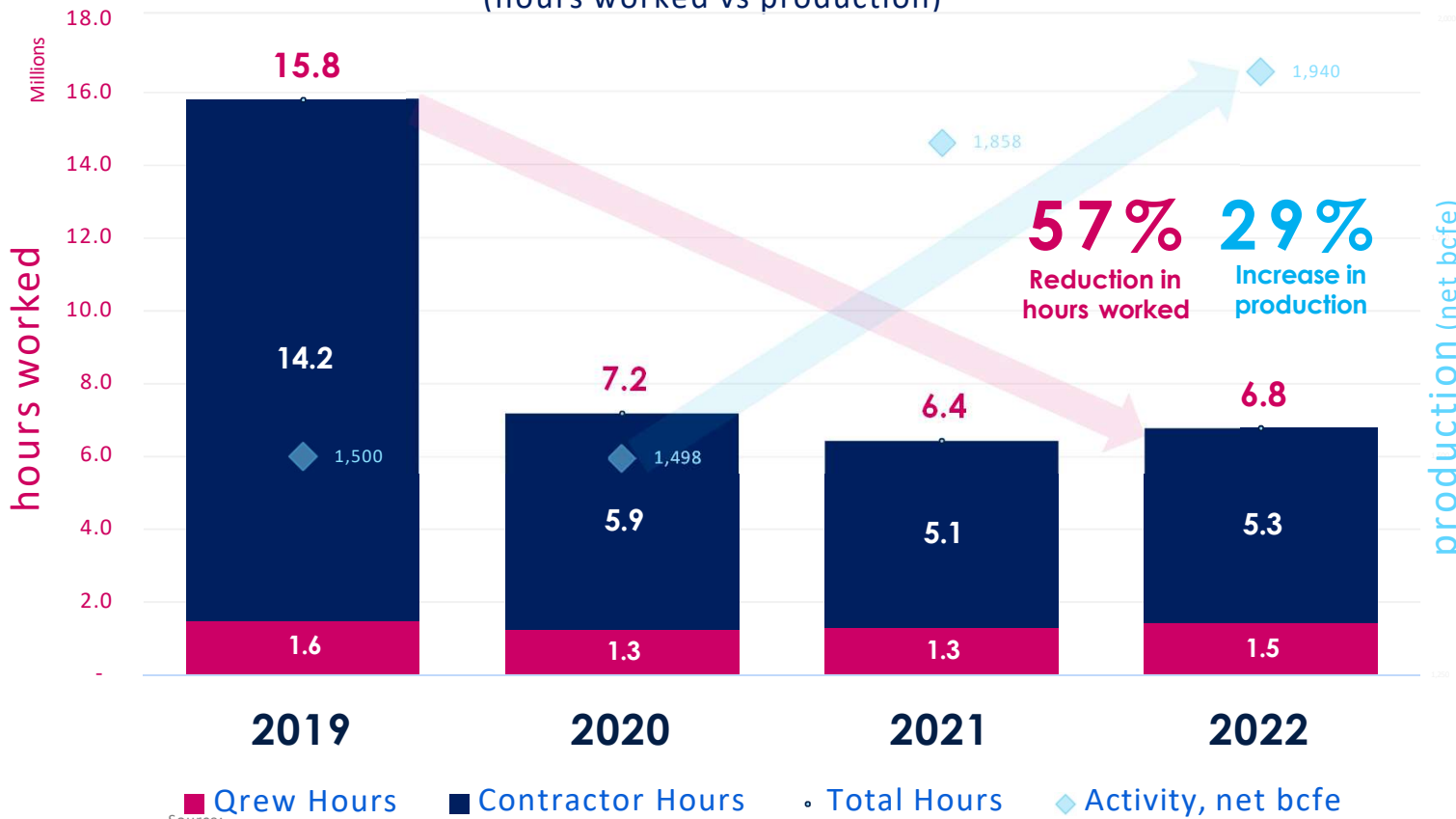


We have seen a large increase in Organizational Efficiency... Benchmarked against EQTLegacy2019



First phase of efficiency centered on “evolving” the organization (2019-2020), second phase focused on doing more work

Organizational Efficiency Inputs & Outputs
(hours worked vs production)



86%
Improvement in Organizational Efficiency

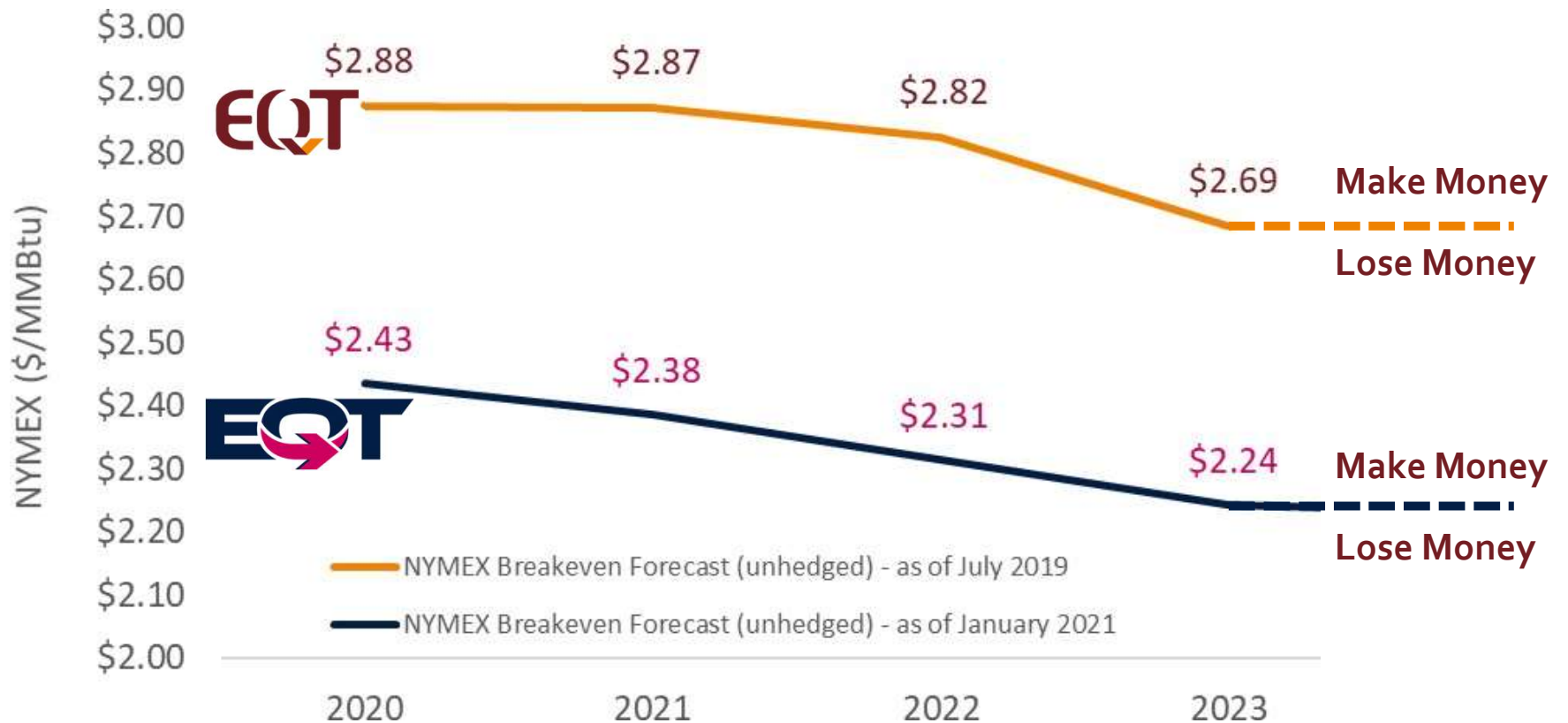
Source:

Our capital efficiency improved significantly...

Every penny of savings translates to \$20MM in FCF



“FCF Breakeven” Cost Structure



July Forecast based on Q2 2019 guidance model (FM_2019.07.19_v2 (Q2 Earnings-5-year Strip)); forecast not provided beyond 2023
 January forecast based on 2021 business plan with updated strip pricing as 1/6/2021 (Corp_Model_2020.01.13_v2)

Our asset performance has seen a step-change in improvement

We are now realizing the full impact of productivity improvements from our operational overhaul



Operational Overhaul:

Implementation of best practices and process standardization has driven:

~98%
Production uptime

&

~40%
Improvement in Marcellus EURs

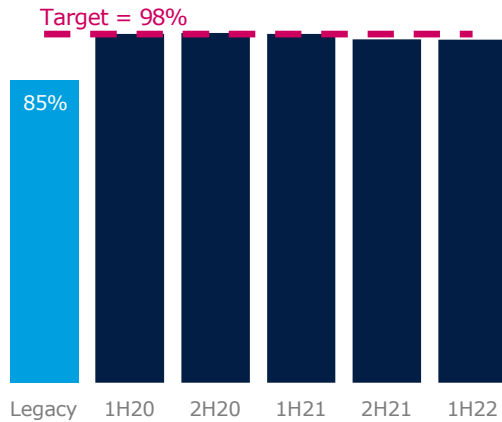
Increased EURs
+ Lower Well Costs
= Improving F&D

Maximizing Production Uptime

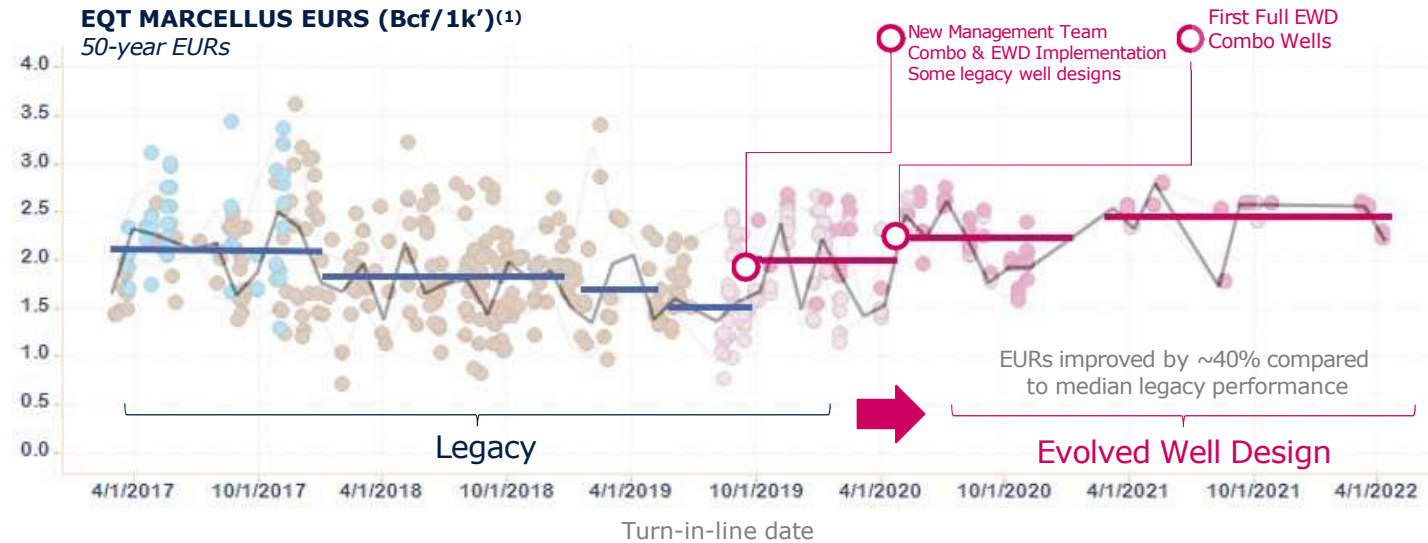
Modern Well Design & Standardization

Repeatable Results & Value Creation

PRODUCTION UPTIME



EQT MARCELLUS EURS (Bcf/1k')⁽¹⁾ 50-year EURs



1. EURs and reserve information are audited by Netherland, Sewell & Associates, Inc. (NSAI), an independent consulting firm.

And our stock price has rebounded...

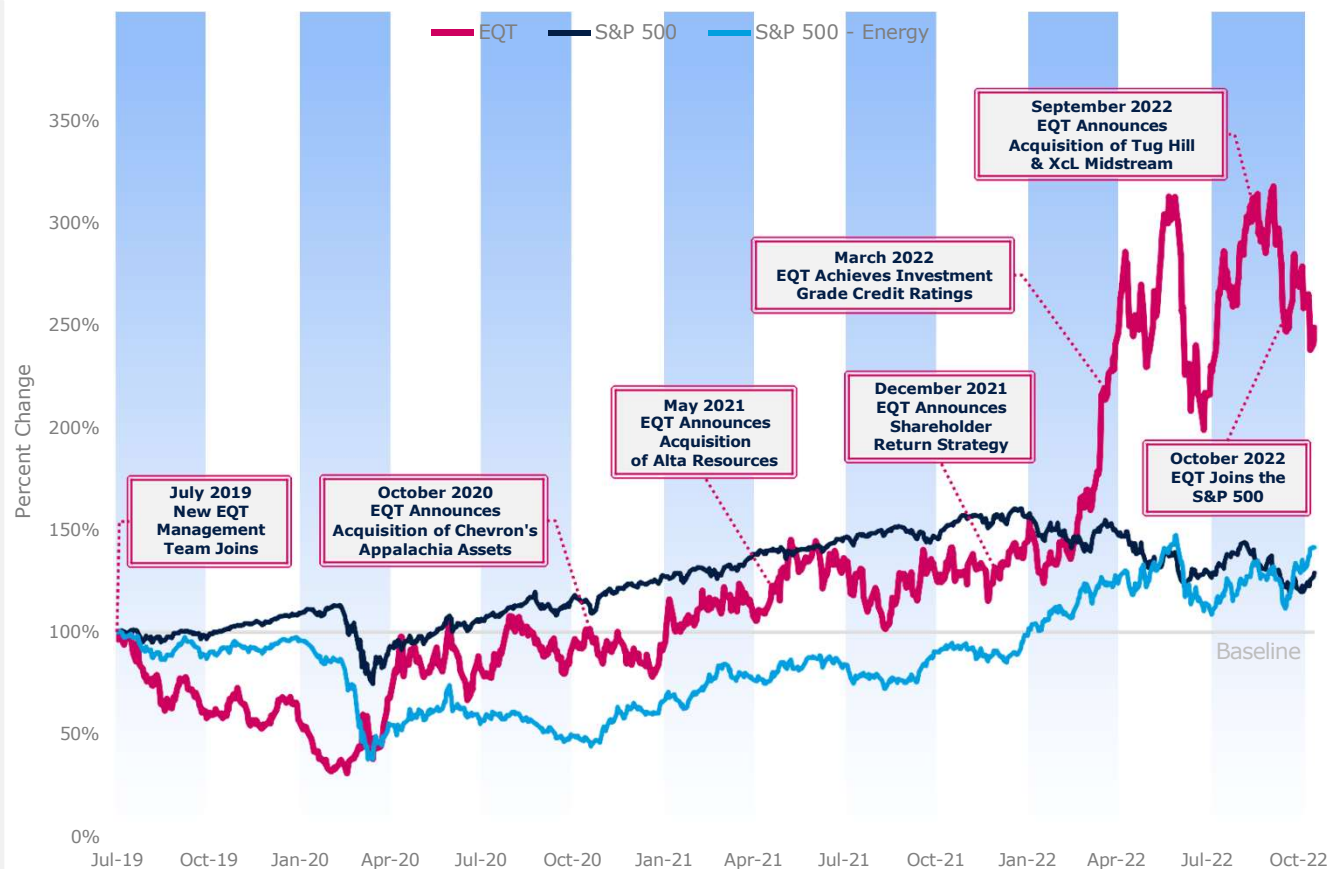
EQT's addition to S&P 500 reflects culmination of multi-year plan execution



A STRONGER, MORE SUSTAINABLE EQT

SINCE MANAGEMENT JOINED EQT:

- > Executed accretive acquisitions and improved cost structure, reducing corporate breakeven⁽¹⁾ from ~\$2.90/MMBtu to ~\$2.15/MMBtu
- > Improved Marcellus EURs by ~40% compared to legacy performance
- > Sustainable cash flow supported by ~1,800 net⁽¹⁾ locations with <\$3.00/MMBtu breakeven requirements; Tug Hill acquisition adds ~300 net locations
- > Drove material balance sheet improvement; targeting 1.0-1.5x leverage⁽²⁾ at \$2.75/MMBtu gas prices
- > Established & executing on shareholder return strategy:
 - \$4.0 B of debt reduction in '22-'23
 - \$2.0 B share repurchase authorization
 - \$0.60/share fixed annual dividend



1. Defined as the Henry Hub prices needed to generate positive free cash flow under a maintenance production plan; assumes (\$0.50) average differential and excludes cash taxes. Average through 2027 pro forma of Tug Hill and XCL Midstream acquisition.
 2. Non-GAAP measure. See appendix for definition.



RF Fall Workshop

August 2023

My Background

Our Transformation

Culture Strategy

Questions



Our Purpose:

Provide energy security for the world and lower global emissions

Our Mission:

Deliver cheaper, more reliable, cleaner energy to the world

Our Vision:

Become the operator of choice for all stakeholders

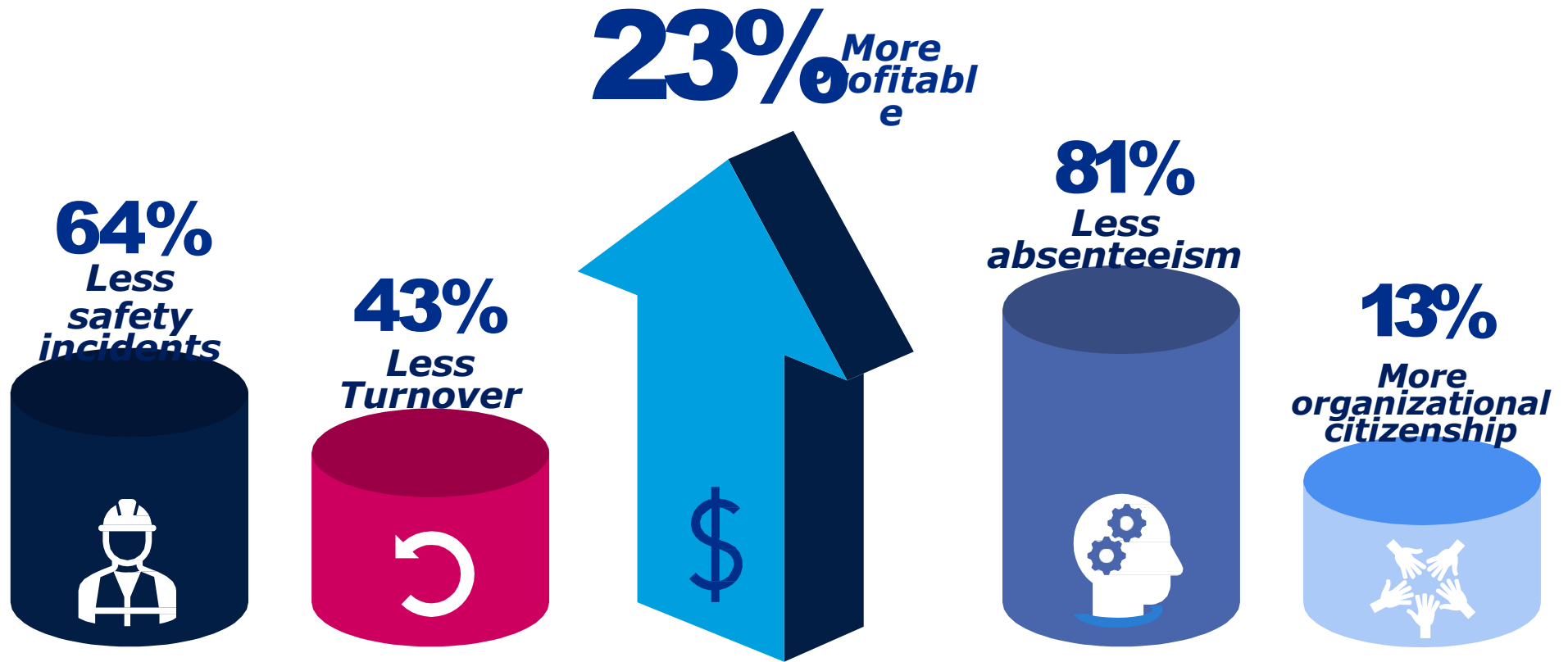
Our Values:

Trust, Teamwork, Heart, Evolution



Culture can contribute to peer-leading results

Highly engaged companies most often produce better results¹



1. Gallup 2020 study: Business outcomes for Top quartile of engagement scores as compared to all organizations (112,312)

Culture: Qrew Culture Programs



We align programs to our strategy; they guide our “shaley” culture

Mission Alignment

“What”

Qrew Metric Program



Plan and Align with total transparency

FOCUS Program **The Way We Work** **ESG Program**

“How”

Plan2Pay Program **Evolution Machine** **Deal Integration**



Leverage values to set clear operational norms

Booster Program **Learning Program**

“Who”

Badge Program **Performance Program**

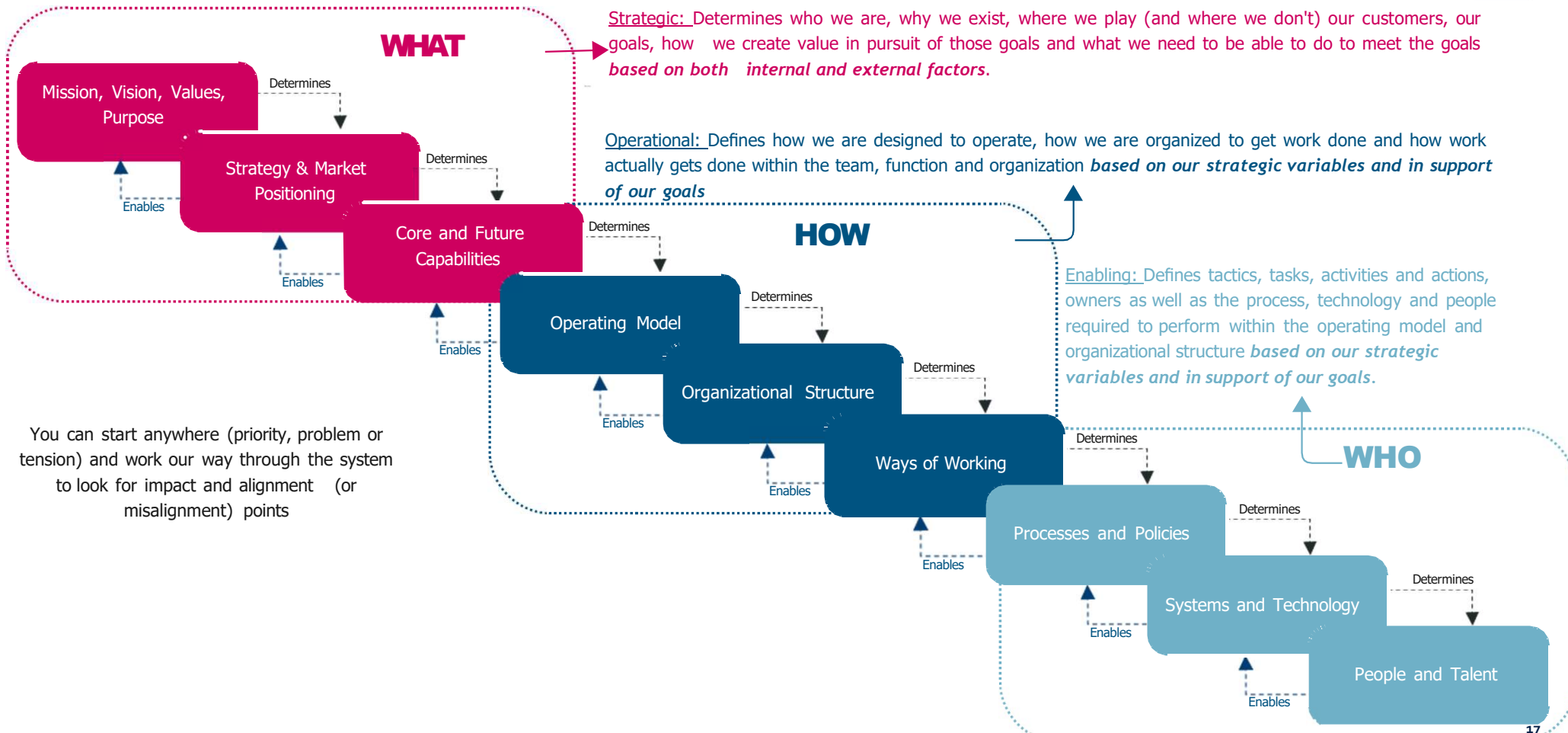


Boost engagement with “happy” employees: Productive, challenged, recognized, and having fun



Aligning culture with the business

A practical model for use in any environment





TRUST

Always doing the right thing.
Doing what you say you will do.



TEAMWORK

Working together toward a common goal. Sharing, respecting and embracing diversity of thought. Understanding customers. Respecting the wrench.



HEART

Caring about what you do (actions). Caring about the relationships you form (impact). Bringing passion and drive to be the best at what you do (attitude).



EVOLUTION

Driving to get better every day. Understanding your environment to prioritize any needed adaption. Being transparent (which enables collaboration that triggers innovation and leads to evolution).



Thank you!







MATT LUAllen

LEAD RESEARCH SCIENTIST FOR EDUCATION
TRANSLATION, UNIVERSITY OF ILLINOIS INFORMATION
TRUST INSTITUTE



Securing in Small Bytes: Tactically Addressing Cybersecurity in Critical Infrastructure

Matthew E. Luallen

Lead Research Scientist
Information Trust Institute, University of Illinois - Urbana

/imagine: securing in small bytes



/imagine: electron management system

Storytelling

- **Electron Management System**
- MITRE Common Weakness Enumeration (CWE)
- Cyber Informed Engineering (CIE)
- ReCIPE In-Person Cooperative Exercise
- Industrial Control System (ICS) Virtualization Testbed
- Generative Artificial Intelligence (AI), NERC, CIE, and MITRE CWE

Electron Management System aka. The Power Grid



- Michael Faraday, Nikola Tesla, Thomas Edison, George Westinghouse, General Electric, utility workers, linemen, electrical engineers, power plant operators, urban planners, U.S. Department of Energy, Federal Energy Regulatory Commission, CISA (ICS-CERT), renewable energy researchers, environmental advocates, policymakers, legislators, manufacturers of electrical equipment, information and communication technology professionals, academics in the field of energy, non-profit organizations, International Energy Agency, NERC, EROs, community leaders, everyday consumers, **you!**
- At least 100x productivity gain

/imagine: electron management system



/imagine: MITRE common weakness enumeration

Storytelling

- Electron Management System
- **MITRE Common Weakness Enumeration (CWE)**
- Cyber Informed Engineering (CIE)
- ReCIPE In-Person Cooperative Exercise
- Industrial Control System (ICS) Virtualization Testbed
- Generative Artificial Intelligence (AI), NERC, CIE, and MITRE CWE

IEEE Security & Privacy Spotlight Article (July/August 2023 edition)

Toward Common Weakness Enumerations in Industrial Control Systems

David M. Nicol | University of Illinois at Urbana-Champaign and Cyber Manufacturing Innovation Institute
Gregory Shannon | Idaho National Laboratory and Cyber Manufacturing Innovation Institute
Monika Akbar | University of Texas at El Paso and Cyber Manufacturing Innovation Institute
Matt Bishop | University of California, Davis and Cyber Manufacturing Innovation Institute
Michael Chaney | Idaho National Laboratory and Cyber Manufacturing Innovation Institute
Matthew Luallen | University of Illinois at Urbana-Champaign and Cyber Manufacturing Innovation Institute

The storyline of MITRE's common weakness enumeration framework illustrates how the security and privacy technical community can collaborate/cooperate with policy makers to advance policy, giving it specifics and filling gaps of technical knowledge to improve security and resilience of critical infrastructure.



on a particular objective called for in the congressional language. One subgroup was tasked with identifying new classes of security vulnerabilities that are likely to arise in industrial control systems (ICS). This group was known as the *Technical Project Team for New Classes of Security Vulnerabilities for ICS (TPT-NCSV)*.

Introduction

The DoE TPT-NCSV leadership recognized the value of existing systems of knowledge about cybersecurity in IT systems [such as MITRE's common weakness enumeration (CWE)], and approached their mission so as to emulate and potentially integrate with those systems, particularly with trends of IT/operational technology (IT/OT) convergence underway.

They adopted the fundamental idea of highlighting areas and activities within ICS that potentially allow for high-consequence vulnerabilities. The focus is not on particular vulnerabilities (e.g., unused web-servers embedded in ICS device operating systems) but on developing descriptions

that apply more generally: classes, categories. The hope is that designers and vendors of ICS hardware, software, and middleware will use these identifications to provide better defense in their designs, and that asset owners will use them to develop more care and defense in the configurations and operations of what the vendors provide. Furthermore, a framework enables the identification and association of new vulnerabilities within a common class; this enables data analysis of vulnerability occurrences, which informs prioritization of mitigation investments. Importantly, TPT-NCSV leadership viewed cybersecurity management and procurement processes as potential sources of vulnerabilities, not just the technology itself in isolation.

The TPT-NCSV committee drew its membership from government organizations, owner/operators of power systems, industry and trade organizations, vendors and manufacturers, academic institutions, and national laboratories. The TPT-NCSV met bimonthly

Toward Common Weakness Enumerations in Industrial Control Systems

David M. Nicol | University of Illinois at Urbana-Champaign and Cyber Manufacturing Innovation Institute
Gregory Shannon | Idaho National Laboratory and Cyber Manufacturing Innovation Institute
Monika Akbar | University of Texas at El Paso and Cyber Manufacturing Innovation Institute
Matt Bishop | University of California, Davis and Cyber Manufacturing Innovation Institute
Michael Chaney | Idaho National Laboratory and Cyber Manufacturing Innovation Institute
Matthew Luallen | University of Illinois at Urbana-Champaign and Cyber Manufacturing Innovation Institute

The storyline of MITRE's common weakness enumeration framework illustrates how the security and privacy technical community can collaborate/cooperate with policy makers to advance policy, giving it specifics and filling gaps of technical knowledge to improve security and resilience of critical infrastructure.

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10194510>

- Equipment and Software Manufacturer and Their Associated Integrators
- Workforce Development
- Organizational Risks and Maturity



CWE is...

CWE™ is a community-developed list of common software and hardware security weaknesses – mistakes that, in proper conditions, could contribute to the introduction of vulnerabilities.

- View all weaknesses related to a category
- Search for a specific weakness type
- Find mapping to other information lists

Vision: CWE informs development, acquisition, and operational efforts resulting in more secure information technology capabilities at lower costs.

The screenshot shows the CWE website homepage. At the top, there is a navigation bar with links for Home, About, CWE List, Scoring, Mapping Guidance, Community, News, and Search. A search bar is located on the right side of the navigation bar. Below the navigation bar, there is a main heading for '2021 CWE Most Important Hardware Weaknesses' with a circular badge indicating '2021 HW' and 'Top 25'. The main content area is divided into several sections: 'CWE List Quick Access' with buttons for 'View CWE' by Software Development, Hardware Design, Research Concepts, and Other Criteria; 'Community Engagement' with links for Hardware CWE SIG, User Experience Working Group, and CWE/CAPEC Board; and 'CWE News' with several news items and a 'More >>' link. A footer note mentions 'Please see our Guidelines for New Content Suggestions For other ways to get involved, contact us'.

'Get Ahead of Boom' Landscape



'Get Ahead of Boom' Landscape



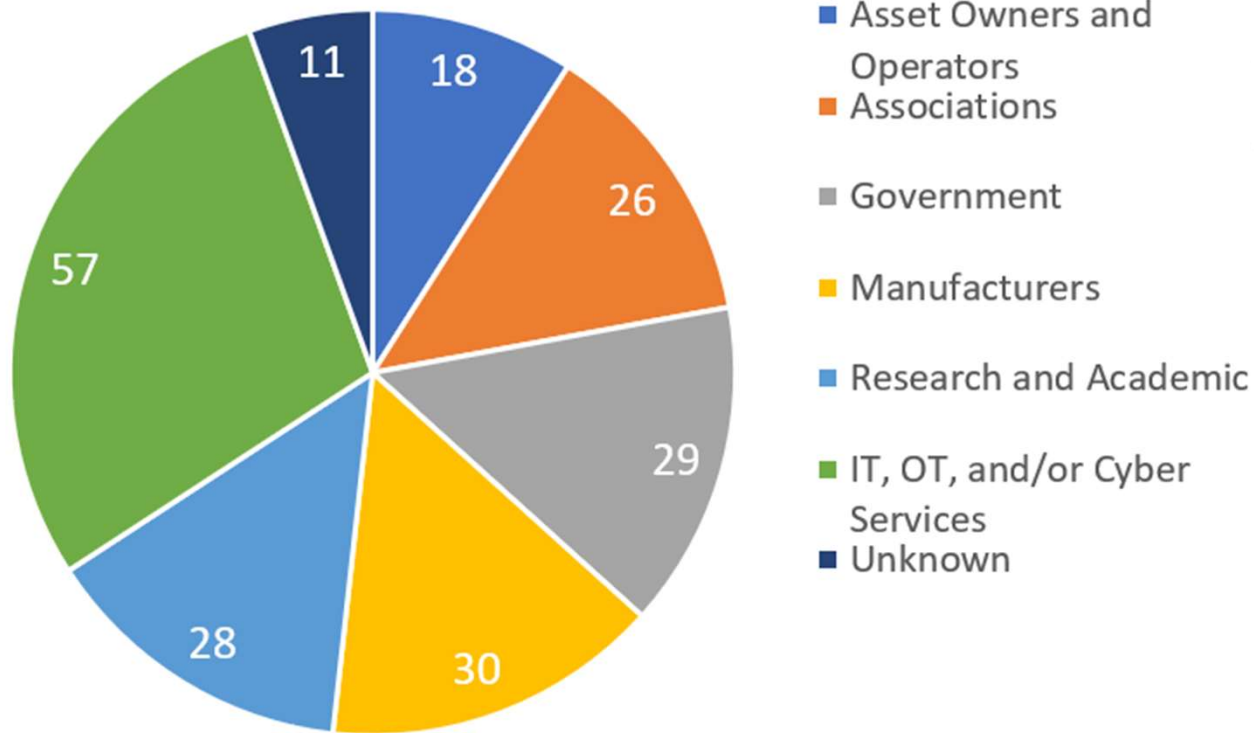
Organization Types

- **Developers and Vendors**
 - Security vendors (involved in ISA 62443, IEC, CISA [ICS-CERT, US-CERT], NIST)
 - Equipment vendors and system integrators
 - Research groups and third-party cybersecurity companies (Dragos, Honeywell, Schneider, Claroty, Bechtel, GE, Nozomi, Schweitzer, Siemens, Xylem, Rockwell, Johnson Controls, CyPhy, Nova, Munio)
- **Manufacturers**
 - Including electrical, ONG, and water
 - Software security tool manufacturers
 - Manufacturers of discrete components
- **Research and Academic Community**
 - Security researchers
 - Academic affiliations (esp. those with a lab that can help process data)
 - Market analyst community
 - Certification labs (non-academic)
- **End Users**
 - Utilities
 - AOOs within each CI sector
- **Policymakers**
- **OSS Community**
- **Other OT SIGs**



SIG Meeting Participants

Total Sig Meeting Participants



Snapshot of CWE → 62443 Mapping Spreadsheet

Small Group	CWE-ID	Abstraction	Relationship	CWE Name	CWE Description	ISA/IEC 62443 Part	Alignment of Mapping (High/Med/Low)	Req. #	CWE Mitigation Phase	62443 Requirement Title	62443 Requirement
3	CWE-654	Base	Child of CWE-657	Reliance on a Single Factor in a Security Decision	A protection mechanism relies exclusively, or to a large extent, on the evaluation of a single condition or the integrity of a single object or entity in order to make a decision about granting access to restricted resources or functionality.	4-1	Low	SD-3	Architecture and Design	SD-3: Security Design Review	A process shall be employed for conducting design review closure security-related issues associated with each signi including but not limited to ...
						4-1	Low	SD-4	Architecture and Design	SD-4: Secure Design Best Practices	A process shall be employed to ensure that secure design applied to the design process. These practices shall be pr design practices include but are not limited ...
3	CWE-655	Base	Child of CWE-657	Insufficient Psychological Acceptability	The software has a protection mechanism that is too difficult or inconvenient to use, encouraging non-malicious users to disable or bypass the mechanism, whether by accident or on purpose.	2-1	Low	4.3.3.6	Policy	Access Control: Authentication	Positively identify network users, hosts, applications, ser transaction so that they can be given the rights and resp they have been granted under account administration
						3-3	Low	SR 1.1	Integration	SR 1.1: Human user identification and authentication	The control system shall provide the capability to identify capability shall enforce such identification and authentica human user access to the control system to support segn accordance with applicable security policies and procedu
						3-4	Low	SD-4	Architecture and Design	SD-4: Secure Design Best Practices	A process shall be employed to ensure that secure design applied to the design process. These practices shall be pr design practices include but are not limited ...
3	CWE-250	Base	Child of CWE-657	Execution with Unnecessary Privileges	The software performs an operation at a privilege level that is higher than the minimum level required, which creates new weaknesses or amplifies the consequences of other weaknesses.	4-1	High	SD-4	Architecture and Design	SD-4: Secure Design Best Practices	A process shall be employed to ensure that secure design applied to the design process. These practices shall be pr design practices include but are not limited ...
						4-2	High	CCSC 3	Documentation	Least Privilege	When required and appropriate, one or more system cor embedded devices, host devices and network devices) sh to enforce the concept of least privilege. Individual syste granularity of permissions and flexibility of mapping those support it. Individual accountability shall be available wh
3	CWE-653	Base	Child of CWE-657	Improper Isolation or Compartmentalization	The product does not properly compartmentalize or isolate functionality, processes, or resources that require different privilege levels, rights, or permissions.	TR99.00.01-2007	This is a Technical Report (not a Standard) and may not be used for mapping	9.1.5		Future Directions	Strong process isolation - protecting pages of main mem assured that it is not modified or observed by any other

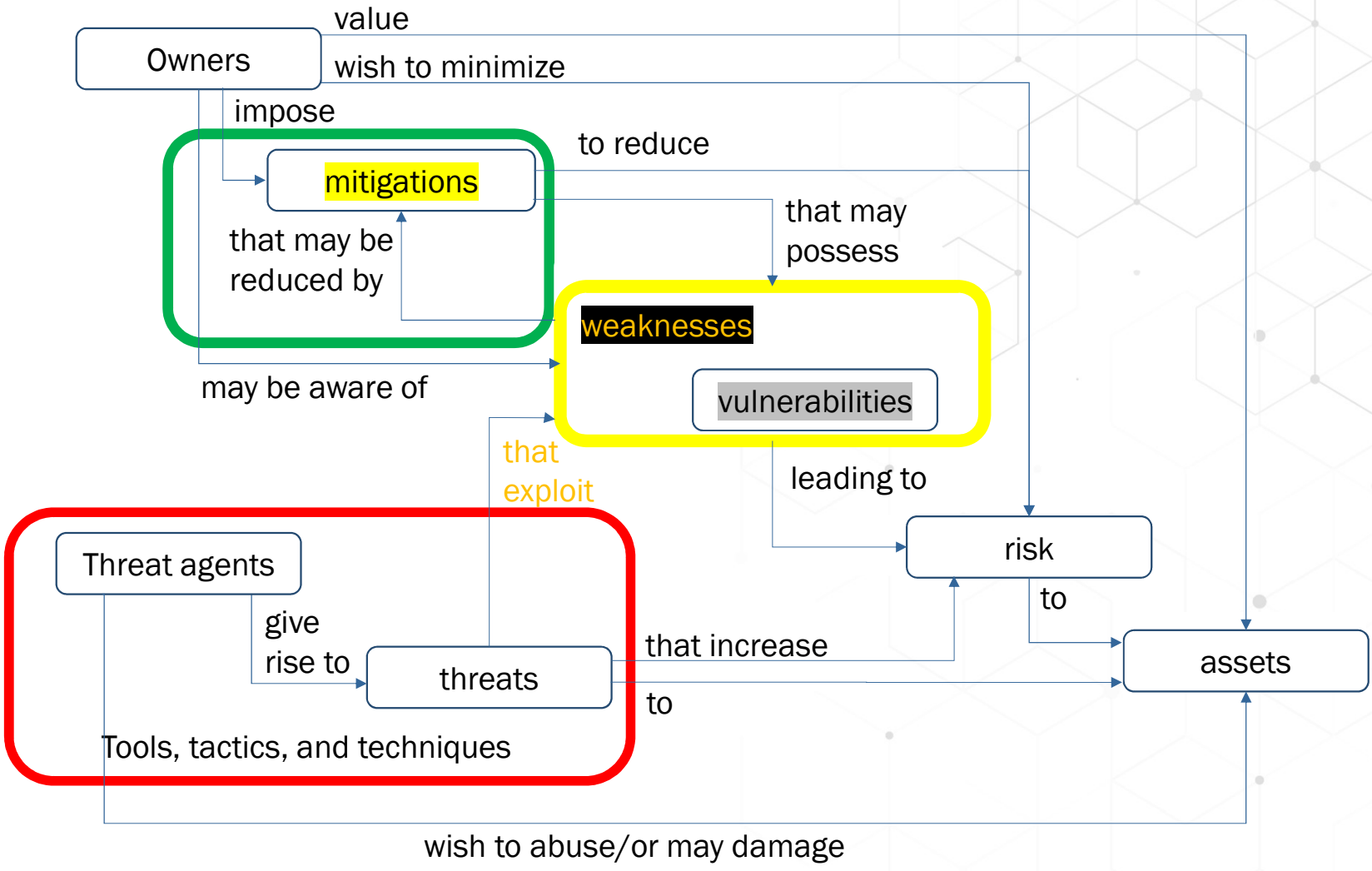


Figure 3: MITRE framework associated ISO/IEC 15408-1:2022 common criteria series fact model

Contextual Fact Model

- **Advanced Persistent Threat (APT) actors** use **CAPEC-100 buffer overflow attack** to exploit **CVE-2023-24014 (Delta Electronics CNCSoft-B)**, a vulnerability tied to **CWE-787 (Out of Bounds Write)** inside of CWE Category 1366 ICS Communications: Frail Security in Protocols. To mitigate this risk to critical ICS/OT systems, organizations implement **"Network Segmentation"** to reduce impact as prescribed in the **ISA 62443 Parts 3-3, 4-1, 4-2, NERC CIP-005, NIST CPG (2.F)**, ensuring proper data flow control and reducing the likelihood of successful exploitation.
- **Threat agent tools, tactics and techniques** applied to **vulnerabilities** categorized by **weaknesses** associated with **mitigations** to reduce asset risk linked to **requirements among guidance, advisories, standards and frameworks**.
- Owners / operators address the weaknesses to manage business risk
- Product developers and service providers enhance their offerings to address weaknesses in support of the owner / operators



/imagine: cyber informed engineering

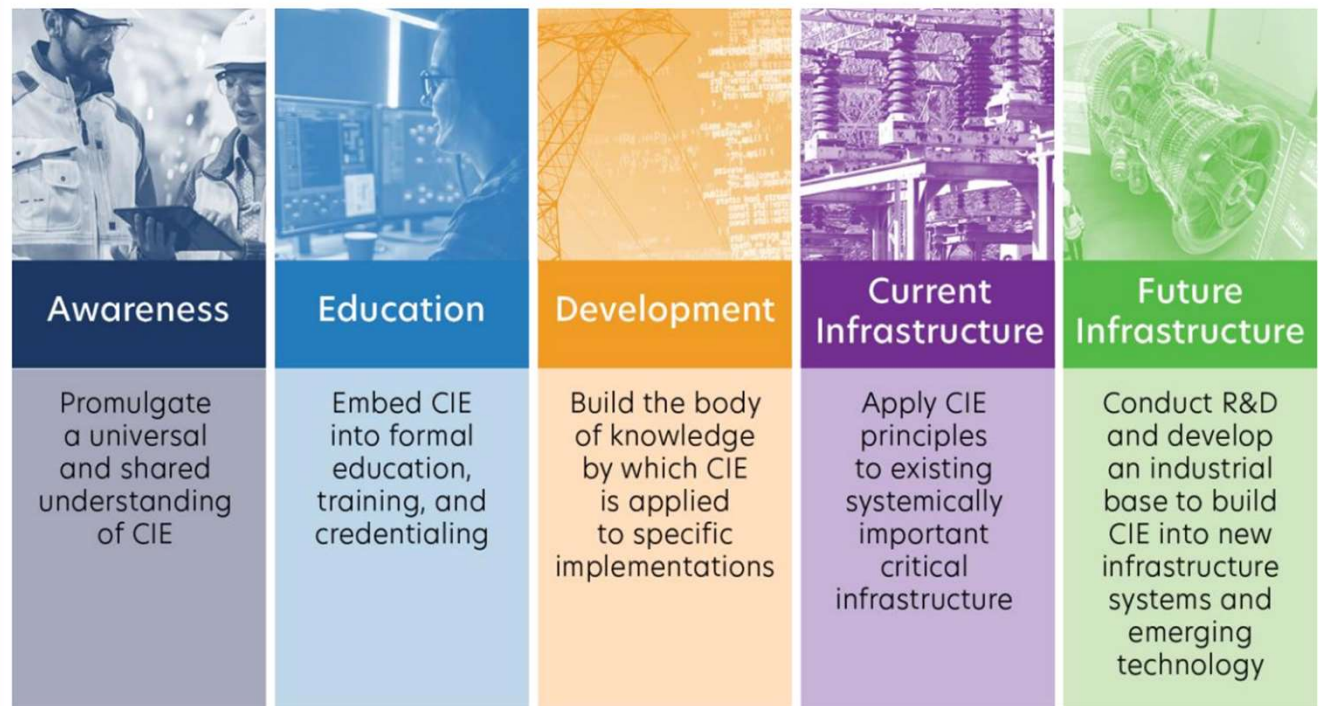
Storytelling

- Electron Management System
- MITRE Common Weakness Enumeration (CWE)
- **Cyber Informed Engineering (CIE)**
- ReCIPE In-Person Cooperative Exercise
- Industrial Control System (ICS) Virtualization Testbed
- Generative Artificial Intelligence (AI), NERC, CIE, and MITRE CWE

Pillars of Cyber Informed Engineering

- Addressing high consequence cyber impacts is included in the design criteria

Figure 1. National Cyber-Informed Engineering Strategy



https://inl.gov/content/uploads/2023/07/FINAL-DOE-National-CIE-Strategy-June-2022_0.pdf

CIE Implementation Guide, p. 150

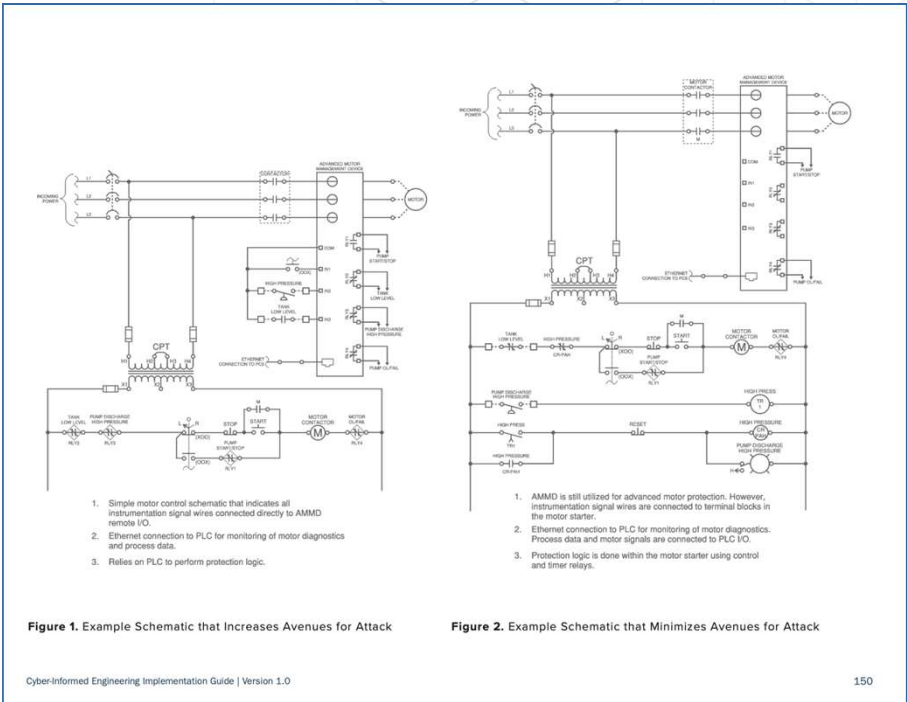
- Design out vulnerabilities

1. Simple motor control schematic that indicates all instrumentation signal wires connected directly to AMMD remote I/O.
2. Ethernet connection to PLC for monitoring of motor diagnostics and process data.

3. Relies on PLC to perform protection logic.

1. AMMD is still utilized for advanced motor protection. However, instrumentation signal wires are connected to terminal blocks in the motor starter.
2. Ethernet connection to PLC for monitoring of motor diagnostics. Process data and motor signals are connected to PLC I/O.

3. Protection logic is done within the motor starter using control and timer relays.



https://inDigitallibrary.inl.gov/sites/sti/sti/Sort_67122.pdf

CIE Practitioners' Workshop

- (G & M discussion) How can we make our presentation practical and informative for researchers and even the larger audience?
 - Research papers have an abstract
 - Start with an abstract to understand and possibly quantify risk for the research and maybe even quantify risk for the implementation phase (and beyond)
- 3 hours to a quick PoC and 13 hours to the current format with tables and a more refined narrative. **All code is generative AI using prompts.**
- CWE = Common Weakness Enumeration
CVE = Common Vulnerabilities and Exposures
Model and Temperature = gpt-3.5-turbo-16k, 0.2

Abstract

- User inputs abstract and the generative AI identifies the technology used
- Generative AI uses this identified technology to associate CWEs with abstract
- Iteration is run 3 times and CWEs in 2 or more are kept

```
def determine_technology(abstract):
    tech_query = ("Based on the provided abstract, identify the type of hardware, technology, system and software that
    "What type of IT and OT systems may be in use? What type of system components are common? Be very det
    "Provide the response in the very specific categories of hardware, technology, systems, software, IT/

    messages = [
        {"role": "system", "content": "You are a helpful assistant, interpret the abstract and provide the results requ
        {"role": "user", "content": f"The abstract is: {abstract}"},
        {"role": "assistant", "content": tech_query}
    ]
```

Abstract: Cup Company manufactures a variety of thermoformed plastic cups and other food service goods. Cup engineers design and maintain the tooling utilized in the thermoforming manufacturing lines. Thermoforming employs air pressure and vacuum tooling to supply suction to a plastic sheet, forcing it onto the walls of a female mold cavity in the shape of the final product. Cup desires that the vacuum tooling employed within the thermoforming process be analyzed in terms of airflow efficiency, followed by measures to improve the efficiency. Analyzing and redesigning the tooling to improve vacuum airflow efficiency can lead to a reduced cycle time and thus an increased production rate. Cup identified the mold cavity assembly as the area to be evaluated and improved. To arrive at a solution, the airflow through the original cavity was analyzed using fluid dynamics, and the resistance to airflow through the cavity was determined by use of a physical experiment that measured the flow rate through the cavity. Design modifications within the mold cavity were tested using Computational Fluid Dynamic (CFD) software, to yield visual representations of flow conditions. Significant changes have been incorporated into a prototype, which was manufactured by Cup's machine shop. Testing of the prototype, in the physical experiment, showed a 39% improvement at one-third the operating pressure and satisfies all the project goals, and is recommended for implementation. KEYWORDS: thermoforming, airflow efficiency, mold cavity , computational fluid dynamics, CFD

Submit

```
cwe_query = ("I need help associating the abstract and identified technology with MITRE CWE. "
    "List the top 10 MITRE CWE weaknesses that apply in the format of 'CWE-XXX, CWE-YYY, ...'
    "Do not provide any other information.")
```

Generate a report

- Output recommendation in a specific format
 - Terms to use
 - Report format
 - Role of generative AI

```

if consistent_cwes:
    next_query = f"""
    Please provide the details and perform the following with the following CWEs in HTML format: {', '.join(consist
    It is very important to associate the impact of the MITRE CWEs, and the concept of CPP, SRDI, and CEEQ with the
    It is very important when referencing CWEs include the concepts of a cyber physical passport (CPP), secure rese
    Cyber Physical Passport (CPP) stores protected metadata following the entire lifecycle of a software or physica
    Secure Research and Development Infrastructure (SRDI) is a novel use of virtual containers to allow the secure
    Cybersecurity, Energy and Emmissions Quantification (CEEQ) is a novel risk, energy, and carbon interdependency
    Secure Defensible Architecture is a mathematically proven approach to cybersecurity using existing frameworks s
    Provide recommendations based on CWE, CPP, SRDI, CEEQ and SDA to make the original abstract secure today and in
    Include the specific MITRE att&ck TTPs the adversary may use to impact the CWEs.
    For each CWE, wrap the information in a <div> with alternating styles:
    the first with a background of light gray (`#f2f2f2`) and the next with a white background (`#ffffff`), and so
    Inside these <div>s, format the report as:
    - <div style='background-color: #f2f2f2; padding: 10px;'>
      <p><b>CWE number</b>: ...</p>
      <p><b>CWE impact</b>: ...</p>
      <p><b>MITRE ATT&CK TTPs</b>: ...</b>
      <p><b>Abstract and/or technology association</b>: ...</p>
      <p><b>SDA, CPP, SRDI, CEEQ associations</b>: ...</p>
      <p><b>Recommendations</b>: ...</p>
    </div>
    - <div style='background-color: #ffffff; padding: 10px;'>
      ...
    </div>
    Then provide a summary at the end wrapped in a <p> tag discussing the overall results and the relationship to c
    """

    messages = [
        {"role": "system", "content": "You are a cybersecurity analyst with engineering skills."},
        {"role": "user", "content": f"The abstract is: {abstract}. The identified technology or system is: {technol
        {"role": "user", "content": next_query}
    ]
  
```

Sample report narrative

- Categorized by CWE, attack TTP, and mitigations
- ['CWE-20', 'CWE-306', 'CWE-89', 'CWE-200', 'CWE-119', 'CWE-78', 'CWE-434']
- A few pennies for our quick thoughts, 4.3

CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

CWE Impact: This CWE occurs when a program writes to or reads from a memory buffer beyond its boundaries, leading to buffer overflows or underflows. It can result in memory corruption, crashes, or the execution of arbitrary code.

MITRE ATT&CK TTPs: T1059 - Command and Scripting Interpreter, T1136 - Create Account, T1190 - Exploit Public-Facing Application

Abstract and/or Technology Association: CWE-119 can be associated with the abstract as it involves analyzing and redesigning the tooling used in the thermoforming process. If the tooling does not properly handle memory buffers, it can be vulnerable to buffer overflow or underflow attacks.

SDA, CPP, SRDI, CEEQ Associations: Implementing secure coding practices, such as bounds checking and input validation, can be part of a Secure Defensible Architecture (SDA). A Cyber Physical Passport (CPP) can store metadata related to memory buffer handling mechanisms used in the manufacturing process. Secure Research and Development Infrastructure (SRDI) can ensure that proper memory buffer handling techniques are integrated into the tooling design and development process. Cybersecurity, Energy, and Emissions Quantification (CEEQ) can consider the impact of CWE-119 on energy consumption and emissions associated with potential attacks.

Overall, the analysis of the provided CWEs in relation to the abstract and technology/system highlights several potential vulnerabilities and associated impacts. These vulnerabilities can be exploited using various MITRE ATT&CK TTPs, which an adversary may employ to compromise the security and integrity of the thermoforming manufacturing process.

To address these vulnerabilities and secure the efforts today and in the future, the following recommendations can be implemented:

- Implement strict input validation mechanisms to prevent CWE-20 (Improper Input Validation) vulnerabilities.
- Ensure proper authentication mechanisms are in place to prevent CWE-306 (Missing Authentication for Critical Function) vulnerabilities.
- Implement secure coding practices, such as input sanitization and parameterized queries, to prevent CWE-89 (SQL Injection) vulnerabilities.
- Implement access controls and encryption mechanisms to prevent CWE-200 (Information Exposure) vulnerabilities.
- Implement proper bounds checking and input validation to prevent CWE-119 (Improper Restriction of Operations within the Bounds of a Memory Buffer) vulnerabilities.
- Use secure coding practices, such as input sanitization and parameterized commands, to prevent CWE-78 (Improper Neutralization of Special Elements used in an OS Command) vulnerabilities.
- Implement strict file type validation and restrict execution permissions on uploaded files to prevent CWE-434 (Unrestricted Upload of File with Dangerous Type) vulnerabilities.

By addressing these vulnerabilities and following the recommendations, the researcher can enhance the security of the thermoforming manufacturing process, protect against potential attacks, and ensure the integrity and efficiency of the production system.

Total Input Tokens Used: 3213

Total Output Tokens Used: 8337

Total Cost: \$0.0430

Connect with external dataset (CVEs in CWE)

- Retrieve records from NIST associated with CWEs
- Place CWEs into a fact tree view based upon number of CVEs in each
- CWE-119 (most CVEs)
 - Translate to an engineer why this matters for the process in 5 words
 - Data corruption, unauthorized access, system crash.
- > 40,000 CVEs

```

resultsPerPage = 2000 # maximum allowed by NVD
global_vulnerabilities = [] # global list to accumulate all vulnerabilities

for cwe in consistent_cwes:
    totalResults = resultsPerPage # initialize totalResults to resultsPerPage so the while loop starts
    startIndex = 0

    while startIndex < totalResults:
        # Make a GET request to retrieve the JSON data for each CWE
        url = f"https://services.nvd.nist.gov/rest/json/cves/2.0?cweId={cwe}&resultsPerPage={resultsPerPage}&startIndex={startIndex}"

```



CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Certain languages allow direct addressing of memory locations and do not automatically ensure that these locations are valid for the memory buffer that is being referenced. This can cause read or write operations to be performed on memory locations that may be associated with other variables, data structures, or internal program data.

As a result, an attacker may be able to execute arbitrary code, alter the intended control flow, read sensitive information, or cause the system to crash.

Digging deeper into realm of CVE/CWE

- Low complexity, network exploitable vulnerabilities among the CWEs

```
In [40]: def extract_access_vector(vulnerability):
cvssMetricV2 = vulnerability.get('metrics', {}).get('cvssMetricV2', [{}])
return cvssMetricV2[0].get('cvssData', {}).get('accessVector')

def extract_access_complexity(vulnerability):
cvssMetricV2 = vulnerability.get('metrics', {}).get('cvssMetricV2', [{}])
return cvssMetricV2[0].get('cvssData', {}).get('accessComplexity')

# Extract the 'cve' column from the 'no_duplicates' DataFrame
global_vulnerabilities = no_duplicates['cve'].tolist()

low_complexity_network_vulnerabilities = [
    vuln for vuln in global_vulnerabilities
    if extract_access_vector(vuln) == 'NETWORK'
    and extract_access_complexity(vuln) == 'LOW'
]

print("Number of low complexity network vulnerabilities:", len(low_complexity_network_vulnerabilities))
```

```
Number of low complexity network vulnerabilities: 23240
```

Low complexity, network exploitable CWE

- CWE-89 with nearly 1,300 CVEs in 2022-2023

- ~~CWE-119~~

```
# Create a DataFrame with the number of vulnerabilities for each CWE and year
vulnerabilities_count = pd.DataFrame({
    'CWE': vulnerabilities_by_cwe.keys(),
    'Total': [len(vulns) for vulns in vulnerabilities_by_cwe.values()],
    'Pre-2020': [len(vulns) for vulns in vulnerabilities_by_year['pre-2020'].values()],
    '2021': [len(vulns) for vulns in vulnerabilities_by_year['2021'].values()],
    '2022': [len(vulns) for vulns in vulnerabilities_by_year['2022'].values()],
    '2023': [len(vulns) for vulns in vulnerabilities_by_year['2023'].values()],
})

print(vulnerabilities_count)
```

	CWE	Total	Pre-2020	2021	2022	2023
0	CWE-20	4606	3665	458	101	0
1	CWE-119	4101	3957	81	4	1
2	CWE-78	1965	909	398	216	12
3	CWE-434	1230	502	282	153	65
4	CWE-200	3784	3437	145	74	1
5	CWE-306	698	286	115	80	2
6	CWE-89	8379	5608	798	857	442

CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.

Recommendation (PoC)

- Recommendation based upon on analysis performed.

```
print(f"Total Cost: ${total_input_cost + total_output_cost:.4f}")
print(response.choices[0].message['content'].strip())
```

Total Cost: \$0.0043

Based on the provided abstract, the research engineer should be aware of the following threat summary:

1. CWE-89 (SQL Injection): This vulnerability allows an attacker to manipulate the SQL queries used in the Cup Company's tooling design process. It can lead to unauthorized access, data leakage, or even complete system compromise. To engineer out this vulnerability, the research engineer should implement secure coding practices, such as using parameterized queries or prepared statements, to prevent malicious SQL injection.

2. CWE-119 (Buffer Overflow): Although only 5 CVEs have been reported, buffer overflow vulnerabilities can have severe consequences. An attacker could exploit this weakness to execute arbitrary code, potentially compromising the entire system. The research engineer should ensure that proper input validation and boundary checks are implemented during the design phase to prevent buffer overflow vulnerabilities.

These weaknesses can impact the thermoforming process described in the abstract by allowing an attacker to manipulate the tooling design, potentially leading to product defects, compromised production rates, or even equipment damage. To address these weaknesses, the research engineer should:

1. Implement secure coding practices: Ensure that all input data is properly validated and sanitized to prevent SQL injection attacks. Use parameterized queries or prepared statements to separate data from code.



/imagine: recipe in-person cooperative exercise

Storytelling

- Electron Management System
- MITRE Common Weakness Enumeration (CWE)
- Cyber Informed Engineering (CIE)
- **ReCIPE In-Person Cooperative Exercise**
- Industrial Control System (ICS) Virtualization Testbed
- Generative Artificial Intelligence (AI), NERC, CIE, and MITRE CWE

ReCIPE In-Person Training / Exercise



- Two-day, **team-based event** held at UIUC in August
 - National Guardsmen and women, Electric Cooperatives, IOUs, Government Agencies
- Rotational 40m – 60m increments
 - **Hands-on ICS/OT Training, Hands-on ICS/OT Exercise, Debrief**
 - Based upon real scenarios leveraging **MITRE Caldera**
- Training and Exercises
 - Pre-exercise training on Incident Response Planning and Asset Inventory
 - Provide connections with people to know how to expand your team when/if necessary (**mutual aid**)
 - Purple teaming (blue defense while learning red techniques)
 - Operating while compromised
 - **Using generative AI (to develop the exercise, and as first level support)**

IOWA STATE
UNIVERSITY

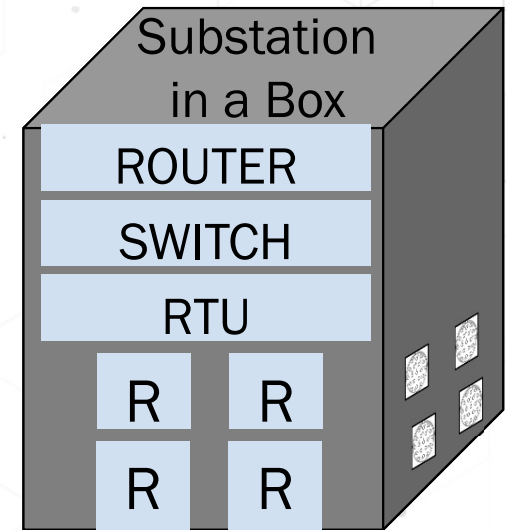
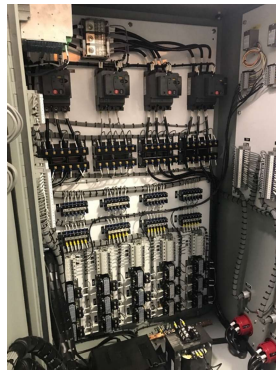
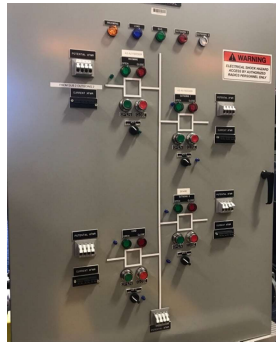


UNIVERSITY OF
ILLINOIS
URBANA - CHAMPAIGN

Rapid Attack Detection, Isolation and Characterization System

[RADICS Physical Testbed]

- Tactical and strategic preparation prior to incident
- Validation of processes and workflows before they are needed
- Real assessment of operational impacts, control efficacy, mitigations, and value of deployed security products



Researching Exercise Elements to Include

Level	Attack Technique	Description	Estimated Cost of Response	Mitigation	Estimated Cost of Mitigation
0	Open-Source Intelligence Gathering	Gathering information about the target through publicly available sources	N/A	Implement data protection measures and reduce the amount of sensitive information available in public sources	\$1,000 - \$10,000
1	Spearphishing	Sending a malicious email or link to trick the target into downloading malware or revealing sensitive information	\$10,000 - \$150,000	Implement email filtering and user training programs to detect and prevent phishing attacks (key: people)	\$5,000 - \$100,000
2	Exploitation	Taking advantage of a vulnerability in the system to gain access or execute malicious code	\$25,000 - \$200,000	Regularly apply software patches and updates to address known vulnerabilities (key: asset inventory and mgmt.)	\$5,000 - \$50,000
3	Lateral Movement	Moving within the network to gain access to additional systems and sensitive data	\$50,000 - \$500,000	Implement network monitoring, segmentation and logging tools to detect and respond to suspicious activity (key: segmentation and monitoring)	\$10,000 - \$100,000
4	Data Exfiltration	Stealing sensitive data from the system	\$100,000 - \$1,000,000	Encrypt sensitive data to prevent unauthorized access (key: MFA)	\$5,000 - \$50,000
5	Ransomware	Encrypting sensitive data and demanding a ransom to restore access	\$500,000 - \$5,000,000	Implement regular backups and disaster recovery plans (key: kept up to date)	\$10,000 - \$100,000
6	Disabling a Substation	Disrupting the operation of a substation by using an additional communication channel on a relay, compromising a HMI, or pivoting via an engineering laptop	\$1,000,000 - \$10,000,000	Implement security measures for all communication channels and regularly monitor network activity for suspicious activity (key: span ports and response)	\$50,000 - \$500,000

Costs are estimates based upon variety of sources, including industry reports, surveys, and case studies



/imagine: industrial control system virtualization testbed

Storytelling

- Electron Management System
- MITRE Common Weakness Enumeration (CWE)
- Cyber Informed Engineering (CIE)
- ReCIPE In-Person Cooperative Exercise
- **Industrial Control System (ICS) Virtualization Testbed**
- Generative Artificial Intelligence (AI), NERC, CIE, and MITRE CWE

Project Goals (ICS Virtualization Testbed)

The project will create a fully virtualized ICS testbed, replicating real-time hardware interactions and unprecedented fidelity, overcoming existing constraints in container synchronization and hardware-specific coding. Our virtualized system, hosted on the cloud, will provide an "effectively hands-on" experience, accommodating multiple concurrent users. Leveraging our prior research and experience with such educational and research platforms, we aim to develop and validate an enhanced platform paving the way for a radical shift in the methodologies used for research and education within the ICS sphere.

- **Virtual hands-on (cloud)**
- **Unprecedented fidelity (simulated hardware interactions)**
- **Increased scalability (cloud, concurrency)**
- **Academics, professionals, and researcher (who cares)**
- **Cyber Informed Engineering (wide impact and accessibility)**

Seeking members for the stakeholder working group



/imagine: generative artificial intelligence,
nerc, cie, and mitre cwe

Storytelling

- Electron Management System
- MITRE Common Weakness Enumeration (CWE)
- Cyber Informed Engineering (CIE)
- ReCIPE In-Person Exercise
- Industrial Control System (ICS) Virtualization Testbed
- **Generative Artificial Intelligence (AI), NERC, CIE, and MITRE CWE**

NERC Reliability Standards, CIE Implementation Guide, and MITRE CWE combined with OpenAI

- AI having a seat at the table with the drafting teams? ... in the board room?

The screenshot shows the MITRE CWE website. The main heading is "2023 CWE Top 25 Most Dangerous Software Weaknesses". Below this, there is a search bar and a list of categories for viewing CWEs: Software Development, Hardware Design, Research Concepts, and Other Criteria. A table at the bottom lists files:

Name	Date Modified
cwe_latest.pdf	Sep 12, 2023 at 3:24 PM
RSComp...eSet.pdf	Sep 12, 2023 at 3:06 PM
Sort_67122.pdf	Today at 11:02 AM

The screenshot shows the cover page of the "Reliability Standards for the Bulk Electric Systems of North America" document. The title is prominently displayed in the center. Below the title, it says "Updated August 10, 2023". At the bottom, there is a logo for "RELIABILITY | ACCOUNTABILITY" and the address: "3133 Inverness Road NE, Suite 400, North Tower, Atlanta, GA 30328".

The screenshot shows the cover page of the "Cyber-Informed Engineering Implementation Guide" document. The title is "Cyber-Informed Engineering Implementation Guide" with "Version 1.0" below it. The date "AUGUST 7, 2023" is also present. At the bottom, there is a "PURPOSE" section that describes the principles of Cyber-Informed Engineering (CIE) and outlines questions that engineering teams should consider during each phase of a system's lifecycle.

<https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf>

https://indigitallibrary.inl.gov/sites/sti/sti/Sort_67122.pdf

<https://cwe.mitre.org/>

Jupyter Notebook (Python Code, < 100 lines)

```

In [2]: import json
import openai

# Read the API key from the config file
with open('keys.json') as config_file:
    config = json.load(config_file)
    openai_api_key = config['openai_api_key']

In [8]: import os
from pdfminer.high_level import extract_text

def save_pdf_as_txt(pdf_path, txt_path):
    text = extract_text(pdf_path)
    with open(txt_path, 'w') as f:
        f.write(text)

# Specify your directories
pdf_dir = './pdf_data'
txt_dir = './data'

# Ensure the output directory exists
os.makedirs(txt_dir, exist_ok=True)

# Convert all PDFs to text files
for filename in os.listdir(pdf_dir):
    if filename.endswith('.pdf'):
        pdf_path = os.path.join(pdf_dir, filename)
        txt_path = os.path.join(txt_dir, filename.replace('.pdf', '.txt'))
        save_pdf_as_txt(pdf_path, txt_path)

# Read the API key

In [*]: import json
import openai
from llama_index import (
    ---GPTVectorStoreIndex,
    ---SimpleDirectoryReader,
    ---LLMPredictor,
    ---ServiceContext)
from langchain.chat_models import ChatOpenAI
import os

# Read the API key from the config file
with open('keys.json') as config_file:
    config = json.load(config_file)
    openai_api_key = config['openai_api_key']

# Use the API key to initialize the OpenAI library
openai_api_key = openai_api_key

os.environ['TOKENIZERS_PARALLELISM']='true'

documents = SimpleDirectoryReader('./data').load_data()

model_name = 'text-davinci-003'
model_name = 'gpt-4'

# Use the API key to initialize the ChatOpenAI model
predictor = LLMPredictor(llm=ChatOpenAI(temperature=0.2,
                                model_name=model_name,
                                openai_api_key=openai_api_key))

serv_context = ServiceContext.from_defaults(
    llm_predictor=predictor,
    chunk_size=600
)

index = GPTVectorStoreIndex.from_documents(documents)

```

```

index = GPTVectorStoreIndex.from_documents(documents,
                                           service_context=serv_context)

index.storage_context.persist(
    persist_dir='./chunkstorage')

print("Written nodeled data in ./chunkstorage folder")

In [9]: from llama_index import (
    StorageContext,
    load_index_from_storage)

from llama_index.query_engine import RetrieverQueryEngine
import time
import os
import json
import gradio as gr
from gradio import components

# Read the API key from the config file
with open('keys.json') as config_file:
    config = json.load(config_file)
    openai_api_key = config['openai_api_key']

# Use the API key to initialize the OpenAI library
os.environ['OPENAI_API_KEY'] = openai_api_key

# Number of chunks you would like to use for an answer.
# Set to 1 to save money.
n_chunks = 5

# Rebuild storage context from the chunkstorage
storage_context = StorageContext.from_defaults(persist_dir='./chunkstorage')

# Load index
loaded_index = load_index_from_storage(storage_context)
loaded_index.service_context.llm_predictor.llm.model_name = 'text-davinci-003'
int(loaded_index.service_context.llm_predictor.llm)

# Retriever
retriever = loaded_index.as_retriever()
retriever.similarity_top_k = k

# Construct the query engine based on the retriever and response_mode
query_engine = RetrieverQueryEngine.from_args(
    retriever=retriever,
    response_mode='compact')

timestamp = time.strftime("%Y_%m_%d-%H_%M_%S", time.gmtime())
filename = "Llama" + timestamp + ".txt"

if not os.path.exists(filename):
    with open(filename, 'w') as f:
        f.write("User: Welcome to OpenAI chat!\n\n")

def get_response(p):
    response = query_engine.query(p)

    with open(filename, 'a') as f:
        f.write("User:\n" + p + "\n\n")
        f.write("AI:\n" + str(response) + "\n\n")

    return str(response)

iface = gr.Interface(fn=get_response, inputs=components.Textbox(label="Your Prompt"), outputs=components.Textbox(label="Local Results"), launch=True)
iface.launch()

```



Connecting Generative AI with NERC, CIE, and CWE

- Connecting MITRE CWE with NERC CIP
- CWEs provides guidance on how to address categories of vulnerabilities (weaknesses)

```
model='text-davinci-003' temperature=0.0 max_tokens=None additional_kwargs={} max_retries=10
Running on local URL: http://127.0.0.1:7862
To create a public link, set `share=True` in `launch()`.
```

Your Prompt

associate nerc cip-007 with mitre cwe, provide a few examples

Clear Submit

Local Results

NERC CIP-007 is associated with the Mitre Common Weakness Enumeration (CWE) and is related to system security management. Examples of CWEs that are related to NERC CIP-007 include:

- CWE-259: Use of Hard-coded Password
- CWE-307: Improper Restriction of Excessive Authentication Attempts
- CWE-311: Missing Encryption of Sensitive Data
- CWE-312: Cleartext Storage of Sensitive Information
- CWE-326: Inadequate Encryption Strength

Flag

Connecting Generative AI with NERC, CIE, and CWE

- Using a small set of documents and a temperature of 0.0 restricts generative AI hallucinations

```
iface = gr.Interface(fn=get_response, inputs=components.Textbox(label="Your Prompt"), outputs=c  
iface.launch()
```

```
print("Bye bye")
```

```
model='text-davinci-003' temperature=0.0 max_tokens=None additional_kwargs={} max_retries=10
```

```
Running on local URL: http://127.0.0.1:7862
```

```
To create a public link, set `share=True` in `launch()`.
```

Your Prompt

connect protective relay controls with mitre cwe

Clear Submit

Local Results

No, it is not possible to answer the question given the context information and not prior knowledge.

Flag

Connecting Generative AI with NERC, CIE, and CWE

- Prioritized guidance combining NERC reliability standards, CIE, and MITRE CWE
- **Common legal language – the act of compliance is a verb, not a noun and this is guidance.**
- **This is guidance and just showing a capability**

```
model='text-davinci-003' temperature=0.0 max_tokens=None additional_kwargs={} max_retries=10
```

Running on local URL: <http://127.0.0.1:7864>

To create a public link, set `share=True` in `launch()`.

Your Prompt

Using the NERC reliability standards, CIE and MITRE CWE, provide prioritized guidance for addressing transient device security risks.

Clear Submit

Local Results

Prioritized guidance for addressing transient device security risks using the NERC reliability standards, CIE and MITRE CWE includes:

1. Ensure that Transient Cyber Assets are managed in an ongoing manner to ensure compliance with applicable requirements at all times, or in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or a combination of both.
2. Authorize users, locations, and uses of Transient Cyber Assets individually or by group, and limit uses to what is necessary to perform business functions.
3. Utilize security patching, including manual or managed updates, to mitigate software vulnerabilities.



/imagine: two more bits to make a byte

Storytelling

- Electron Management System
- MITRE Common Weakness Enumeration (CWE)
- Cyber Informed Engineering (CIE)
- ReCIPE In-Person Cooperative Exercise
- Industrial Control System (ICS) Virtualization Testbed
- Generative Artificial Intelligence (AI), NERC, CIE, and MITRE CWE

Still 2 more bits to make a byte



/imagine: risky bits designed out

Thank you!

Matthew E. Luallen
Lead Research Scientist

University of Illinois Urbana-Champaign
The Grainger College of Engineering
Information Trust Institute
mluallen@illinois.edu

Those 2 bits of information didn't provide value and may have increased risk, **so they were designed out**



JUSTIN LADNER

PRESIDENT, PENNSYLVANIA AMERICAN WATER



ReliabilityFirst : Parallels and Interdependencies Between Water and Electric Industries

September 2023

Justin Ladner
SVP, President of Pennsylvania American Water

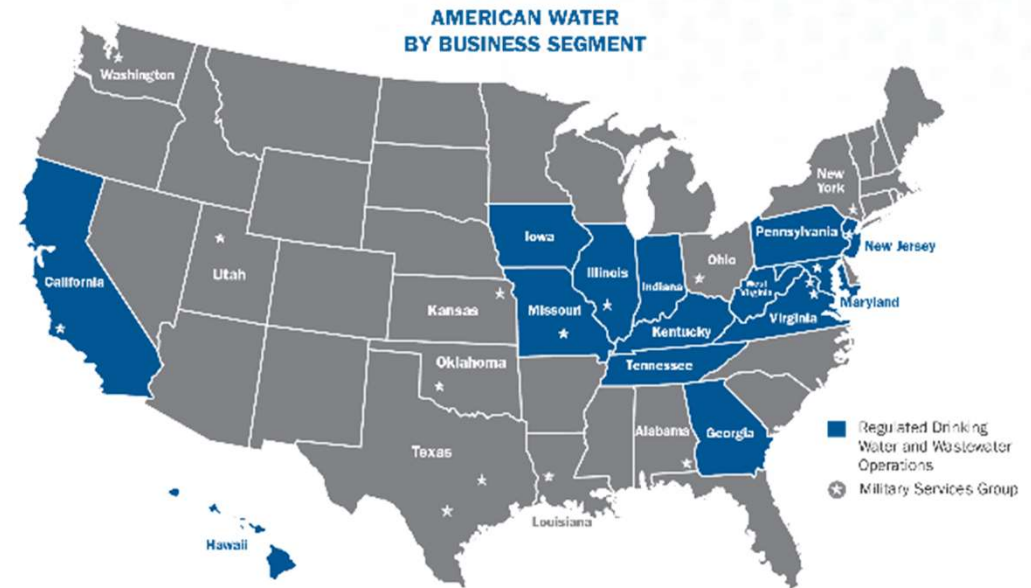
Agenda

- Who is American Water?
- Water/Energy Nexus
- Parallels
 - Water/Wastewater Infrastructure Needs
 - Resiliency/System Hardening
 - Compliance – Emerging Contaminants (PFAS)

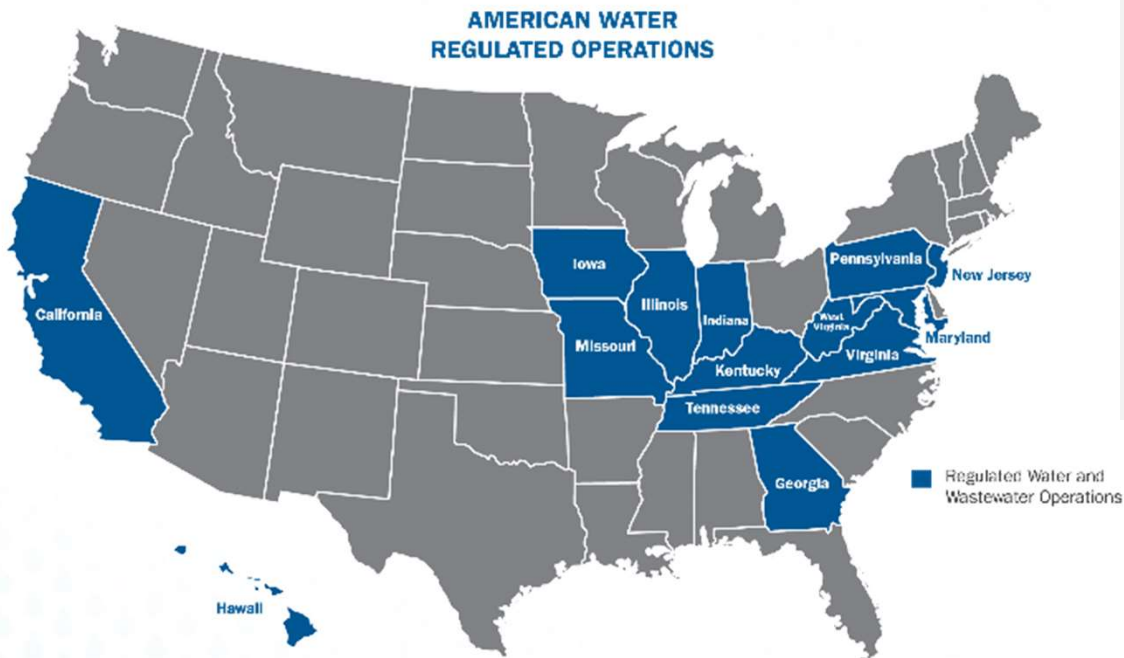
About American Water

We are the largest and most geographically diverse publicly traded water and wastewater service provider in the United States.

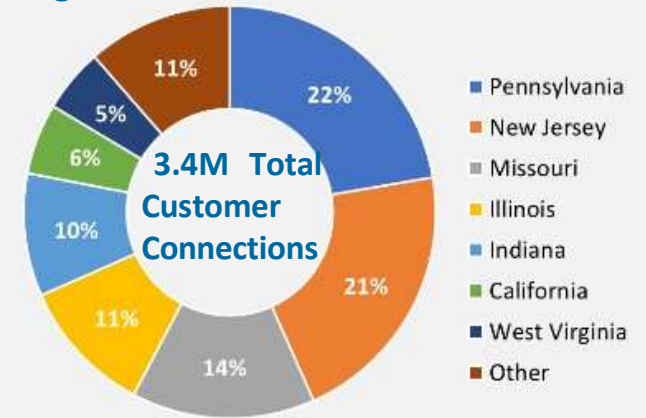
- We serve a broad national footprint and a strong local presence.
- We provide services to approximately 14 million people in 24 states.
- We employ 6,500 dedicated and active employees and support ongoing community support and corporate responsibility.
- We treat and deliver more than one billion gallons of water daily.



American Water – Our Regulated Business at a Glance



Regulated Customer Count

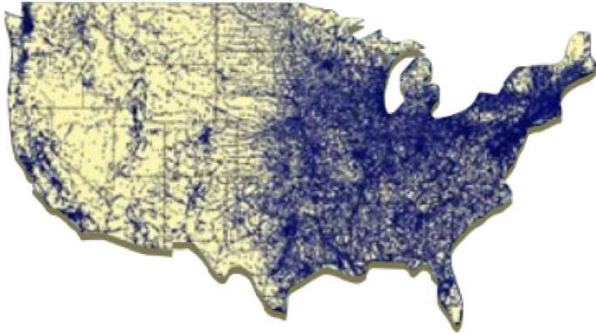


Regulated Operations

- 52,500 miles of pipe
- 560 water treatment plants
- 160 wastewater treatment plants
- 1,100 wells and 73 dams

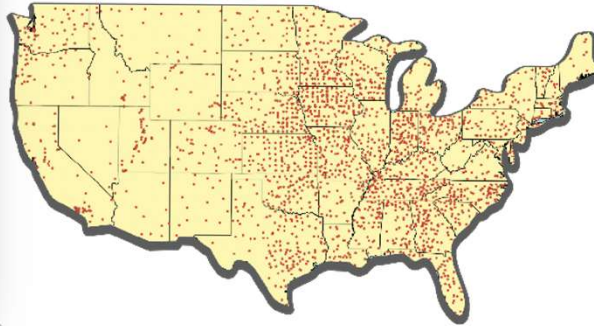
Highly Fragmented Water Industry

Water Utilities



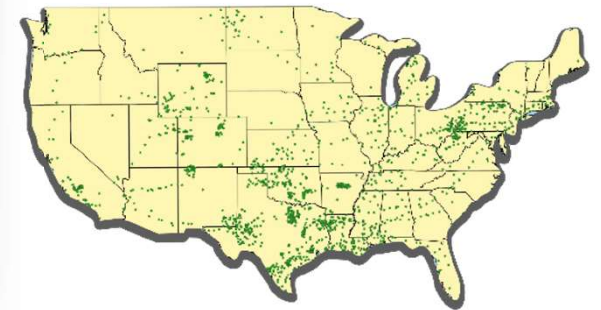
Water Utilities Source: EPA SDWIS
Federal Reports Search
www3.epa.gov/enviro/facts/sdwis

Electric Utilities



Electric Utilities Source: Form EIA-861
detailed data files
www.eia.gov/electricity/data/eia8

Natural Gas Utilities



Gas Utilities Source: EPA F.L.I.G.H.T. Greenhouse
Gas Emissions from Large Facilities
Ghgdata.epa.gov/ghgp/main.do#

Water-Energy Nexus

Water-Energy Interdependencies - Energy

- The nation's water and energy systems are highly interdependent – thermoelectric generation, fuels production, and water treatment.
- Trends: Low Carbon doesn't always = low water (biofuels, carbon capture, nuclear, electrolysis for 'green' H₂)

	Consumption (gal/MWh)		
	Extraction	Processing	Transport
Coal	3–45 ⁷	18	<1 ⁸
Natural Gas	1–12 ⁹	<1	1–3 ¹⁰
Nuclear	18–32 ¹¹	56–87 ¹²	

Source: Meldrum et al. 2013

- On average, 50,000 to 350,000 gallons of water are required to fracture one well in a coalbed formation, while between two million and nine million gallons of water are necessary to fracture one horizontal well in a shale formation (Clark, Horner et al. 2013).

Water-Energy Interdependencies – Water

- Drinking water and wastewater systems account for 3-4% of US energy use
- As much as 40 percent of operating costs for drinking water systems can be for energy.
- Geography dependent – Elevation and distance (Ex. Pittsburgh, Scranton, CA)

Table 2.3. Energy Intensity of Water Treatment and Pumping in California (kWh/MG).

	Low	High	Notes	Reference
Treatment				
Drinking Water Treatment	100	16000	High: Desalination	(CEC 2005)
Wastewater Treatment and Distribution	1100	4600		(CEC 2005)
Pumping				
Water Supply/Conveyance	0	14000	High: Interbasin transfer (State Water Project); Low: Gravity fed	(CEC 2005)
Primary Drinking Water Distribution	700	1200		(CEC 2005)
Recycled Water Distribution	400	1200		(CEC 2005)
Groundwater for Agriculture	500	1500	High: CO River Basin Low: North CA Coast	(CPUC 2011)

Water-Energy Interdependencies – Efficiency/Redundancy Strategies

- System integrity (water loss)
- Technology/Maintenance – ex: Variable Frequency Drive pumps/motors
- Hydraulic engineering studies
- Onsite backup power
- Black Sky Tabletop joint exercises with regulators and utilities



Infrastructure & Resiliency

Aging Infrastructure – Drinking Water



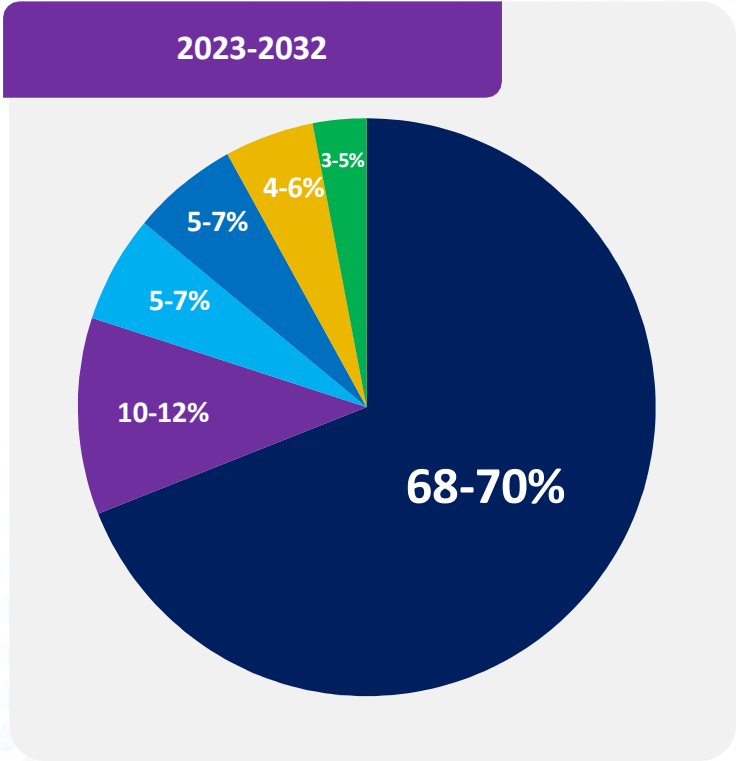
- Nation's drinking water infrastructure system - 2.2 million miles of underground pipes
- The system is aging and underfunded
- Water main break every two minutes
- Estimated 6 billion gallons of treated water lost each day in the U.S.
- This equates to 2.1 trillion gallons of non-revenue water loss per year. The U.S. lost an estimated \$7.6 billion of treated water in 2019 due to leaks
- Some of the nation's oldest pipes were laid in the 19th century
- Pipes laid post-World War II have an average life span of 75 to 100 years and reaching the end of their design life

Aging Infrastructure – Wastewater



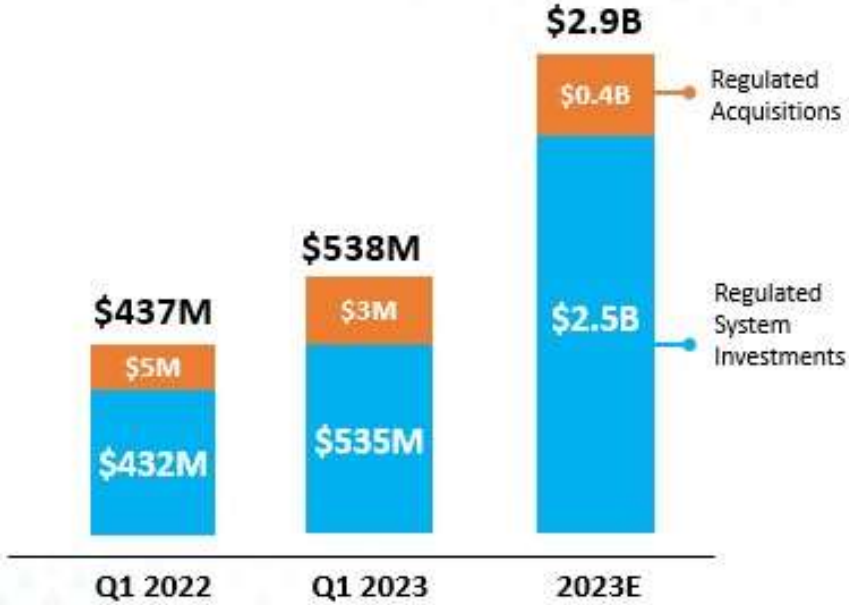
- 16,000 wastewater treatment plants in U.S. are functioning at 81% design capacities
 - 15% have reached or exceeded design Capacity
- Estimates indicate that utilities spent over \$3 billion in 2019
 - \$18 per wastewater customer to replace almost 4,700 miles of pipeline nationwide
- Nation's wastewater footprint includes over 800,000 miles of public sewers and 500,000 miles of private lateral sewers that connect to homes and businesses
- In the U.S. drinking water and wastewater pipes in the ground are on average 45 years old with components more than a century old
- The lifespan expected for wastewater pipes is 50 to 100 years

Regulated Capital Expenditures by Purpose



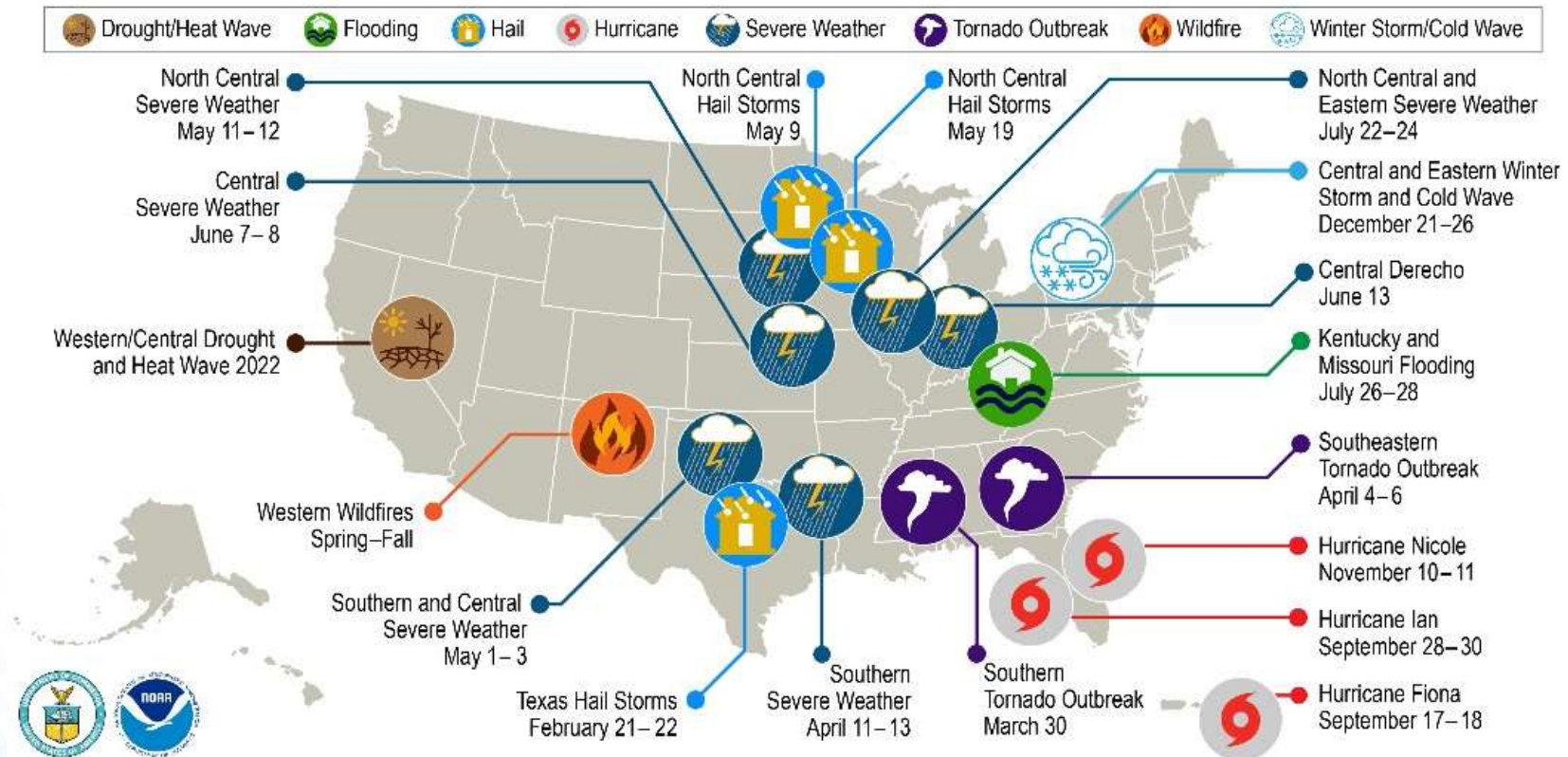
- Infrastructure Renewal
- Resiliency
- Water Quality
- Operational Efficiency, Technology & Innovation
- System Expansion
- Other

Capital Investment



Large-scale Climate Disasters are Varied and Widespread...

U.S. 2022 Billion-Dollar Weather and Climate Disasters



This map denotes the approximate location for each of the 18 separate billion-dollar weather and climate disasters that impacted the United States in 2022.

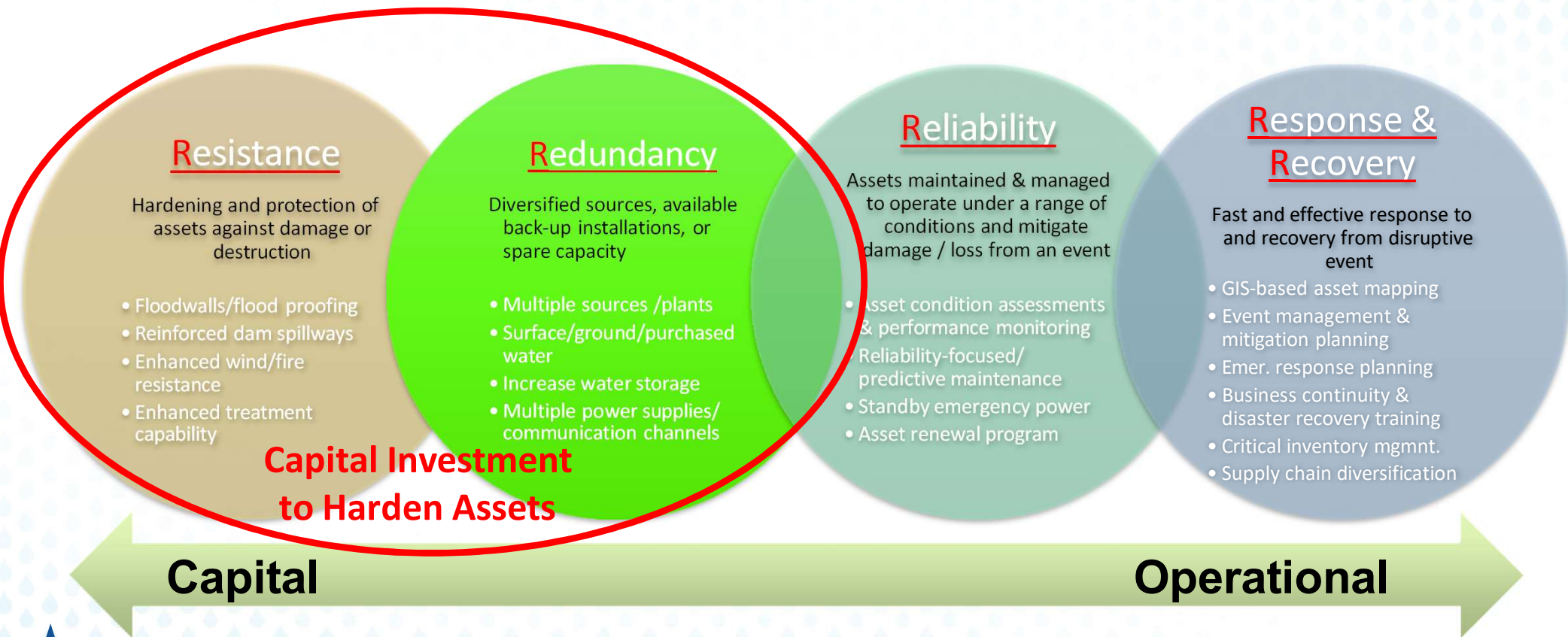
Significant Threats of Concern – *Natural & Man-Made*

- Drought
- Source water contamination
- Flooding
 - Pluvial (flash flood)
 - Fluvial (river/stream overbank)
 - Coastal/Storm Surge
 - Dam/Reservoir Release or Breach
- Hurricanes
- Tornadoes
- Earthquakes/seismic events
- Ice storms/extreme freezing
- Wildfires
- Man-made: Train derailments, Fires, Spills



Resilience Defined & The “Five R’s” of Utility Resilience

An ability to anticipate, absorb, adapt to, and/or rapidly recover from a disruptive event



Reducing Risk by Minimizing Vulnerability



PAAW Dam Projects

- Labyrinth spillways retrofitted into existing dams
- Extends flow area and mitigates spillway failure risk during high rain events

MDAW Mt. Soma Reservoir Project

- 97 million-gallon impoundment which addresses drought risk
- Reduce withdrawals from stream in low flow conditions and reliance on adjacent utility
- Can supply our 5,000 customers with water during a drought of approximately 100 days

Reducing Risk by Minimizing Vulnerability



PAAW – Old Elwood WTP in Floodplain

PAAW WTP Relocation Project

- New treatment plant built ~100-feet higher
- Dual intakes to mitigate single source of supply risk



PAAW – New Elwood WTP built on top of river valley

Reducing Risk by Mitigating Consequence



Shelbyville – Johnson County Operations



2020—Fairland Road transmission main installed, connecting Shelbyville to London Road WTP already serving Johnson County Operations. Adds water source & second WTP, mitigating against the risk of the Blue River WTPs transmission main failing. Also added filter capacity and made high service pump upgrades at London Road WTP.

2021—Replaced backup generators at Orme & Sugar Creek WTPs

PAAW Norristown Water Treatment Plant



Norristown Water Treatment Plant adjacent to Schuylkill River

- 18 MGD capacity water treatment plant serves approximately 33,000 customers in 11 municipalities in Montgomery County, PA
- Most recently expanded/renovated in 1995, including barriers to mitigate flooding in buildings
- Tanks, treatment areas, and administration areas designed / constructed for full protection against 25-year flood event and moderate protection against 100-year flood event
- Minimal flood protection and limited accessibility during 500-year flood event
- Hurricane Ida flooding rose to levels just short of a 500-year flood event at the Norristown WTP

500-year floodway

100-year floodway

Regulatory floodway

PAAW Norristown WTP - Post-Ida Site Conditions



PAAW Norristown WTP - After Action Assessment



- Facility was able to remain in service throughout event – no customers impacted
- Site / building access limited; moderate flooding within treatment plant
- If Schuylkill River flooding had reached the 500-foot event level at Norristown WTP (as happened immediately downstream in Philadelphia) the impacts would have been more consequential
- Additional flood mitigation is now being planned to protect against a 500-year flood event
- Flood protection yielded an estimated **\$25+ million avoided WTP property damage and \$46 million avoided regional economic loss**
 - Estimated \$457 regional economic loss avoided per \$1 invested
 - Estimate based on EPA's water utility economic analysis tool (WHEAT)
 - Analysis assumes facility would have been offline for an estimated 9-days but partial system demands would be met through emergency interconnections



Cybersecurity

Threats and Strategic Objectives

Industry Threats

Cyber-attacks on utilities and critical infrastructure are increasing and more sophisticated

Insider and privileged access threats are increasing

Supply Chain attacks create new challenges

Connected operational devices with embedded technologies continue to expand, as do their vulnerabilities

Phishing landscape is evolving to phone (Vishing) and texting (Smishing)

Attacks targeting ICS and SCADA systems are more frequent

Strategic Objectives



Advance our exchange of threat Information with US Intelligence Agencies and other relevant sectors through automated mechanisms



Educate employees on the evolving cyber security landscape and conduct simulations to validate understanding



Ensure continued compliance with security and evolving data privacy regulations



Understand and mitigate physical/cyber risks through risk management, business continuity planning, simulations and exercises



Continue to deliver on the cyber fundamentals; Patching, Anti-Malware, Privileged Access, and Operational Technology controls



Leverage advanced tools and embedded AI to perform real-time detection and automated responses

Partnerships/Leadership

External Leadership

- Water Sector Coordinating Council
- ASIS Utilities Security Council
- Water ISAC
- J100 Standard Committee
- Process Control System Security (AWWA)

External Programs

- Cyber Security Advisors (CSA)
- Protective Security Advisor (PSA)
- Cyber Information Sharing and Collaboration Program (CISCP)
- Private Sector Clearance Program

CYBERSECURITY FRAMEWORK



**American Water Works
Association**

Dedicated to the World's Most Important Resource®

- **AWWA G430-14 SECURITY PRACTICES FOR OPERATION AND MANAGEMENT**



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM



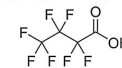
EPA United States
Environmental Protection
Agency



Compliance - PFAS

PFAS Background

- Per- and polyfluoroalkyl substances (PFAS) are man-made synthetic materials used in manufacturing since the 1940's.
- Common uses include nonstick cookware, water repellent clothing, stain resistant fabrics and carpets, firefighting foams, etc.
- They are found today in water, air, fish and soil globally.
- While the use of some of these chemicals has ceased, over 9,000 types of PFAS have been identified and are in use.
- PFAS remain in the environment for an unknown amount of time and bioaccumulate in people.



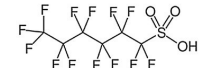
Perfluorobutanoic acid (PFBA)



Perfluorobutane sulfonic acid (PFBS)



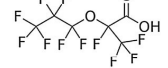
Perfluoroheptanoic acid (PFHpA)



Perfluorohexane sulfonic acid (PFHxS)



Perfluorooctanoic acid (PFOA)



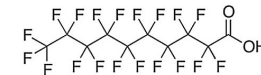
Hexafluoropropylene oxide dimer acid (HFPO-DA or GenX)



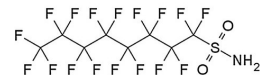
Perfluorononanoic acid (PFNA)



Perfluorooctane sulfonic acid (PFOS)



Perfluorodecanoic acid (PFDA)



Perfluorooctanesulfonamide (PFOSA)

Pennsylvania PFAS Regulations

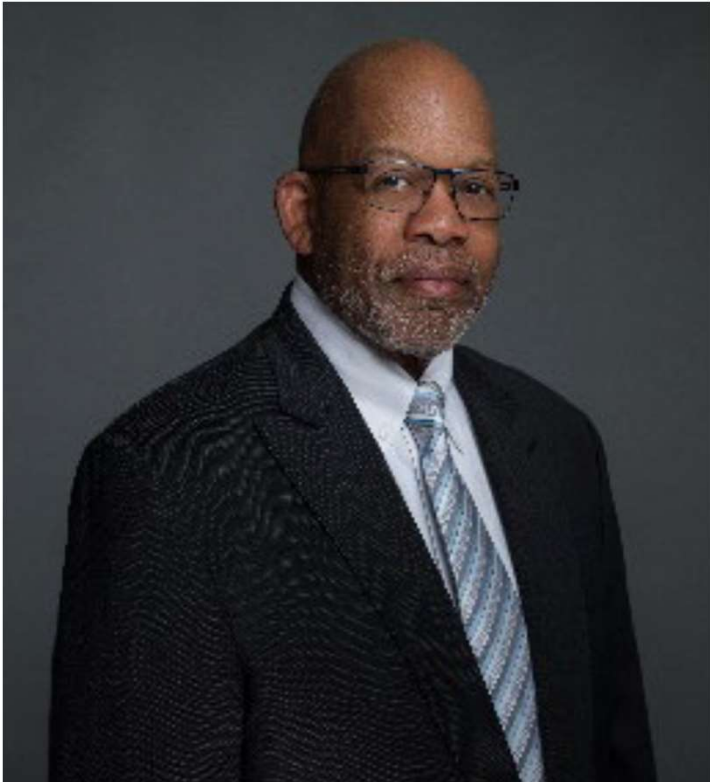
- Passed by the Environmental Quality Board as final at the October 12, 2022 meeting
- Established MCLs/MCLGs for two common PFAS
 - PFOA 14 ng/l; 8 ng/l (ppt)
 - PFOS 18 ng/l; 14 ng/l (ppt)
- Compliance determined by running annual average for each entry point based on quarterly sampling.
- Rule applies to ALL systems. Initial compliance monitoring for systems greater than 350 persons begins Jan. 1, 2024. For smaller systems, Jan. 1, 2025.
- Approves several treatment technologies (others will be considered by DEP)
 - Granular Activated Carbon (GAC)
 - Ion Exchange
 - Reverse Osmosis

PFAS at the Federal Level

- In June 2022, EPA announced new interim health advisories for PFOA and PFOS (Previously 70 ppt for both)
- March 2023 - EPA introduced *proposed* enforceable Maximum Contaminant Level (MCL) regulations for six PFAS found in drinking water – 4.0 ppt (intend to finalize by end of 2023).
- Proposed rule would also require public water systems to:
 - Monitor for these PFAS
 - Notify the public of the levels of these PFAS
 - Reduce the levels of these PFAS in drinking water if they exceed the proposed standards.
- The estimated national cost to install treatment facilities and processes to remove PFOA and PFOS at drinking water facilities to levels required by the U.S. EPA's proposal exceeds \$47 billion*
- On a national basis, more than \$700 million annually for operating costs*

**Data and approach as presented in a recent study conducted by Black & Veatch on behalf of American Water Works Association*

Thank you



KEVIN WALKER

PRESIDENT AND CEO, DUQUESNE LIGHT
HOLDINGS, INC.

PANEL DISCUSSION



Kevin Walker

President & CEO, Duquesne



Stephen DeFrank

Chairman, PA PUC



Lesley Evancho

Chief Human Resources
Officer, EQT



Matt Luallen

Lead research scientist for
education translation, UIUC



Justin Ladner

President, Pennsylvania
American Water

EVENING RECEPTION, 5:00-7:00 PM

SEVENTEENTH FLOOR

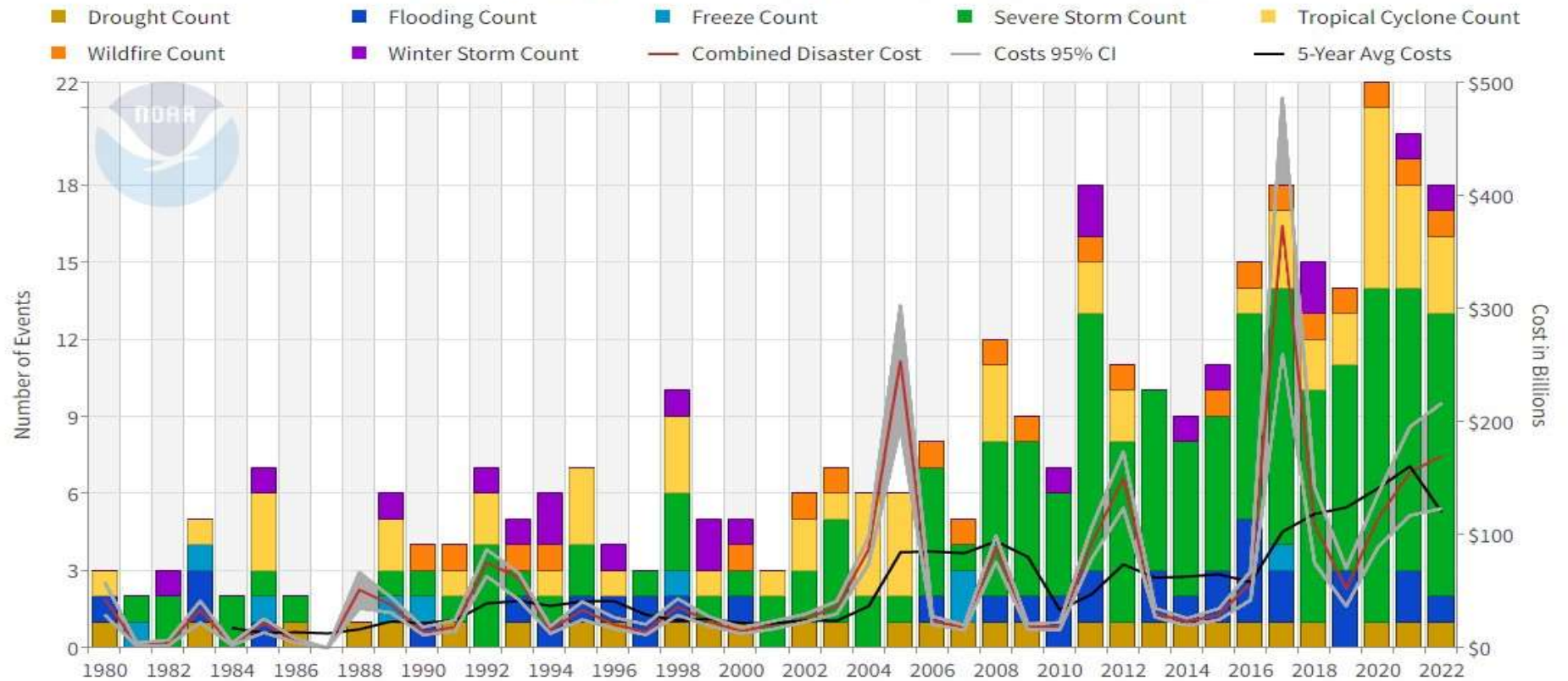
Omni William Penn Hotel
530 William Penn Pl
Pittsburgh, PA 15219



Appendix

...and Increasing in Frequency

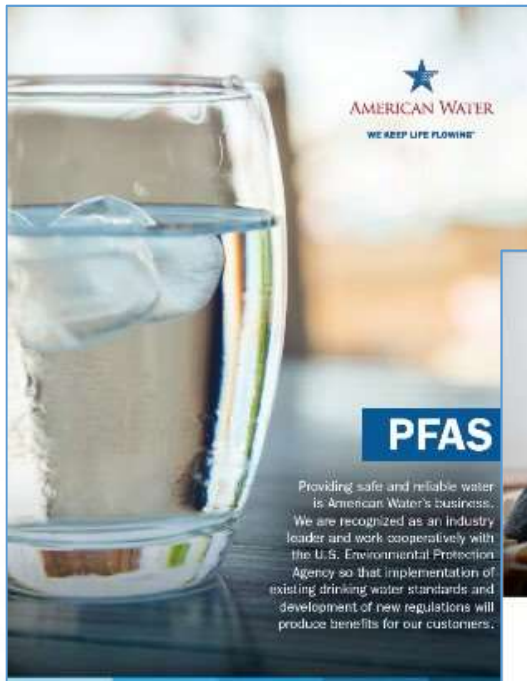
United States Billion-Dollar Disaster Events 1980-2022 (CPI-Adjusted)



Updated: January 10, 2023

Powered by ZingChart

American Water PFAS Brochure



AMERICAN WATER
WE KEEP LIFE FLOWING™

PFAS

Providing safe and reliable water is American Water's business. We are recognized as an industry leader and work cooperatively with the U.S. Environmental Protection Agency so that implementation of existing drinking water standards and development of new regulations will produce benefits for our customers.

COMMONLY ASKED QUESTIONS AND ANSWERS

WHAT ARE PFAS?
Per- and polyfluoroalkyl substances (PFAS) are man-made chemicals historically used in consumer products including cookware (e.g., Teflon™), stain repellents (e.g., Scotchgard™), and waterproofing (e.g., GORE-TEX®). They are also used in industrial applications such as in firefighting foams and electronic production. There are thousands of PFAS chemicals and new products in a constant flow. The most common are perfluorooctanoic acid (PFOA) and perfluorooctane sulfonic acid (PFOS).
Additional information on PFAS from the United States Environmental Protection Agency's U.S. EPA can be found at www.epa.gov/pfas.

HAS U.S. EPA SET DRINKING WATER LIMITS FOR PFAS?
In March 2022, U.S. EPA announced a proposed drinking water regulation to set limits for six PFAS. American Water submitted comments on the proposed drinking water regulation based on our extensive experience in developing and testing treatment for groundwater and surface water, including treatment for PFAS that allows us to meet state standards, and implementing drinking water regulations across our footprint.
Additionally, U.S. EPA has established guidelines for the form of health advisories for PFOA, PFOS, PFBS, and HFOA.
As the U.S. EPA sets new water quality regulations, we will make necessary investments or operational adjustments to comply with the new standards. last updated on 04/24

AMERICAN WATER HAS BEEN ADDRESSING THE PROPOSED DRINKING WATER LIMITS FOR PFAS FOR YEARS. HOW DO WE KNOW THAT?
American Water has been addressing the proposed drinking water limits for PFAS for years. We have been working with the U.S. EPA and state agencies to understand the science and regulatory requirements for PFAS removal. We have been investing in research and development to advance our understanding of PFAS and the best ways to remove them from drinking water. We have been working with our customers to understand their needs and expectations for PFAS removal. We have been working with our regulators to understand the requirements for PFAS removal. We have been working with our industry peers to share best practices and advance the state of the art in PFAS removal technology.

AMERICAN WATER HAS BEEN ADDRESSING THE PROPOSED DRINKING WATER LIMITS FOR PFAS FOR YEARS. HOW DO WE KNOW THAT?
American Water has been addressing the proposed drinking water limits for PFAS for years. We have been working with the U.S. EPA and state agencies to understand the science and regulatory requirements for PFAS removal. We have been investing in research and development to advance our understanding of PFAS and the best ways to remove them from drinking water. We have been working with our customers to understand their needs and expectations for PFAS removal. We have been working with our regulators to understand the requirements for PFAS removal. We have been working with our industry peers to share best practices and advance the state of the art in PFAS removal technology.

PROTECTING PUBLIC HEALTH THROUGH DRINKING WATER STANDARDS FOR PFAS

- American Water supports the United States Environmental Protection Agency's (U.S. EPA) efforts to protect public health by proposing national drinking water standards for PFAS. These standards are a response to the challenges the water industry faces regarding water quality, quantity, and reliability. That's why American Water is committed to being a leader in the U.S. water and wastewater industry and a provider of solutions to these challenges.
- We have already invested and submitted comments regarding the U.S. EPA's proposed drinking water standards for PFAS and the application of a health advisory for PFOA, PFOS, PFBS, and HFOA.

- American Water has already invested in research and development to advance our understanding of PFAS and the best ways to remove them from drinking water. We have been working with the U.S. EPA and state agencies to understand the science and regulatory requirements for PFAS removal. We have been investing in research and development to advance our understanding of PFAS and the best ways to remove them from drinking water. We have been working with our customers to understand their needs and expectations for PFAS removal. We have been working with our regulators to understand the requirements for PFAS removal. We have been working with our industry peers to share best practices and advance the state of the art in PFAS removal technology.
- American Water has already invested in research and development to advance our understanding of PFAS and the best ways to remove them from drinking water. We have been working with the U.S. EPA and state agencies to understand the science and regulatory requirements for PFAS removal. We have been investing in research and development to advance our understanding of PFAS and the best ways to remove them from drinking water. We have been working with our customers to understand their needs and expectations for PFAS removal. We have been working with our regulators to understand the requirements for PFAS removal. We have been working with our industry peers to share best practices and advance the state of the art in PFAS removal technology.

HOW AMERICAN WATER ADDRESSED PFAS IN THE PAST?

- American Water has already addressed PFAS in the past. Here are two examples:
 - Flint, Michigan:** In January 2015, American Water's Michigan Service Group (MSG) began operations to remove PFOA and PFOS from the city's water supply. American Water's MSG team worked with the city of Flint to understand the science and regulatory requirements for PFAS removal. We have been investing in research and development to advance our understanding of PFAS and the best ways to remove them from drinking water. We have been working with the U.S. EPA and state agencies to understand the science and regulatory requirements for PFAS removal. We have been investing in research and development to advance our understanding of PFAS and the best ways to remove them from drinking water. We have been working with our customers to understand their needs and expectations for PFAS removal. We have been working with our regulators to understand the requirements for PFAS removal. We have been working with our industry peers to share best practices and advance the state of the art in PFAS removal technology.
 - California:** American Water has been working with the state of California to understand the science and regulatory requirements for PFAS removal. We have been investing in research and development to advance our understanding of PFAS and the best ways to remove them from drinking water. We have been working with the U.S. EPA and state agencies to understand the science and regulatory requirements for PFAS removal. We have been investing in research and development to advance our understanding of PFAS and the best ways to remove them from drinking water. We have been working with our customers to understand their needs and expectations for PFAS removal. We have been working with our regulators to understand the requirements for PFAS removal. We have been working with our industry peers to share best practices and advance the state of the art in PFAS removal technology.

WHAT IS AMERICAN WATER DOING TO ADDRESS PFAS AND PROTECT OUR CUSTOMERS?

- American Water has a cross-functional team focused on the scientific and regulatory requirements for PFAS removal and ensuring compliance with new standards.
- During the past several years, we have been investing in research and development to advance our understanding of PFAS and the best ways to remove them from drinking water. We have been working with the U.S. EPA and state agencies to understand the science and regulatory requirements for PFAS removal. We have been investing in research and development to advance our understanding of PFAS and the best ways to remove them from drinking water. We have been working with our customers to understand their needs and expectations for PFAS removal. We have been working with our regulators to understand the requirements for PFAS removal. We have been working with our industry peers to share best practices and advance the state of the art in PFAS removal technology.
- We are piloting an advanced water treatment technology during our ongoing investment in our new water treatment plants and existing plants.
- American Water's research group is actively involved in industry-led efforts to advance the science and regulatory requirements for PFAS removal. We have been investing in research and development to advance our understanding of PFAS and the best ways to remove them from drinking water. We have been working with the U.S. EPA and state agencies to understand the science and regulatory requirements for PFAS removal. We have been investing in research and development to advance our understanding of PFAS and the best ways to remove them from drinking water. We have been working with our customers to understand their needs and expectations for PFAS removal. We have been working with our regulators to understand the requirements for PFAS removal. We have been working with our industry peers to share best practices and advance the state of the art in PFAS removal technology.
- U.S. EPA has been invited to remove PFAS compounds from the list of chemicals that have a health advisory water quality.

EXPERTISE

Our Central Laboratory, located in Belleville, IL, is a U.S. EPA-accredited laboratory for PFAS. The Central Laboratory is a PFOA, PFOS, and PFAS Laboratory for U.S. EPA compliance. U.S. EPA compliance will be done with U.S. EPA methods 1631 and 1631C. American Water is also using scientific technology and analytical capabilities, in our research labs, to understand the best ways to remove PFAS from drinking water. We have been investing in research and development to advance our understanding of PFAS and the best ways to remove them from drinking water. We have been working with the U.S. EPA and state agencies to understand the science and regulatory requirements for PFAS removal. We have been investing in research and development to advance our understanding of PFAS and the best ways to remove them from drinking water. We have been working with our customers to understand their needs and expectations for PFAS removal. We have been working with our regulators to understand the requirements for PFAS removal. We have been working with our industry peers to share best practices and advance the state of the art in PFAS removal technology.



WORKING WITH OTHERS ON PFAS

- American Water is active in several national organizations that are helping to shape the future of regulatory and monitoring standards.
 - American Water is a member of the National Association for Safe Drinking Water Act (NASDWA), which has been actively contributing to the development of PFAS standards and regulatory requirements for PFAS.
 - American Water supports regulatory solutions and state and federal legislation in departments of environmental protection, EPA, CDC, American Water Works Association, Water Research Foundation, and other organizations to better understand the science and regulatory requirements for PFAS removal. We have been investing in research and development to advance our understanding of PFAS and the best ways to remove them from drinking water. We have been working with the U.S. EPA and state agencies to understand the science and regulatory requirements for PFAS removal. We have been investing in research and development to advance our understanding of PFAS and the best ways to remove them from drinking water. We have been working with our customers to understand their needs and expectations for PFAS removal. We have been working with our regulators to understand the requirements for PFAS removal. We have been working with our industry peers to share best practices and advance the state of the art in PFAS removal technology.

FOR MORE INFORMATION

For more information, customers can reach the U.S. Environmental Protection Agency's Safe Drinking Water Hotline at 1-800-424-9371.

<https://www.amwater.com/resources/PDF/american-water-PFAS.pdf>





Other slides

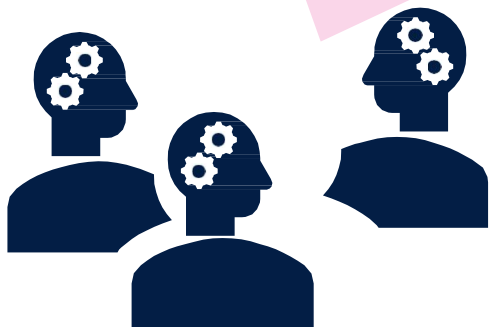


Culture: Qrew Culture Moments















Recognizing our shaley culture, every day

I have a Qrew Culture moment that I'd like to share, related to Teamwork....



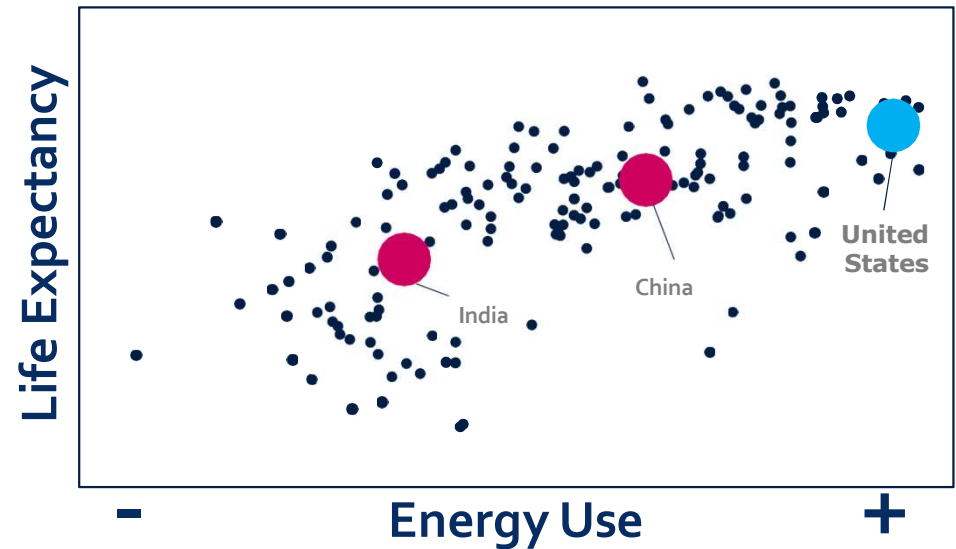
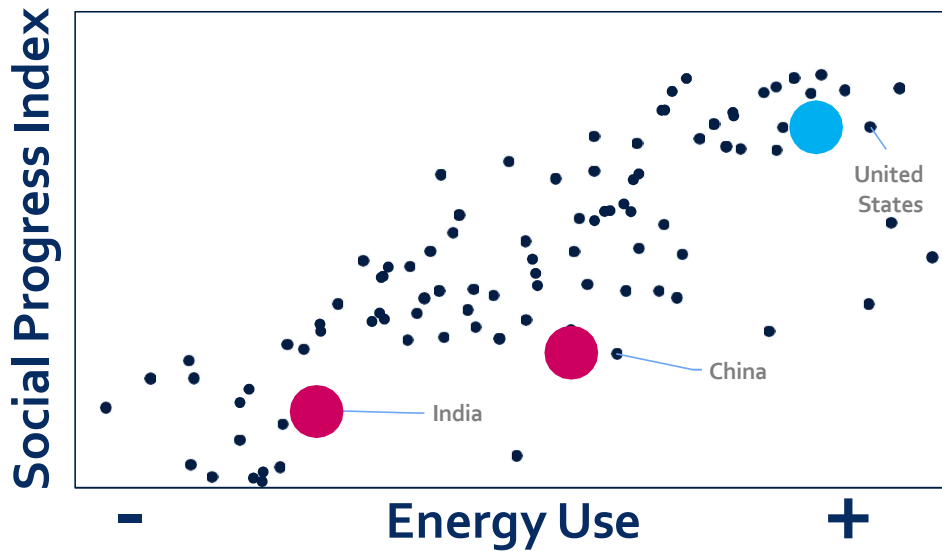
What is it: Couple minutes at the beginning of a meeting describing a situation where our culture was exhibited
Who does it: Meeting Organizer
When: Every meetings with 3+ people

Culture Program	Make it a Culture Moment
 Qrew Metric Program	Talk about a recent "Win"
 Mission Alignment	How have actions aligned with company mission, vision, or higher purpose
 FOCUS Program	Safety moment - incident review, stop work, hazard identification, etc
 ESG Program	Actions taken to strengthen our ESG Performance
 The Way We Work	New tool that was created and how it helps the company
 Plan2Pay Program	Successful outcome related to Project Management
 Evolution Machine	A great solution to a problem
 Deal Integration	A best practice that was identified during integration
 Badge Program	Recognition of a recent display of our values or badge
 Evolve Program	A skill of training that was acquired
 Performance Program	Feedback that was helpful in keeping us on track
 Booster Program	A recent culture booster that made you more engaged



The Driving Force Behind **Our Higher Purpose**

Energy Consumption Drives Human Progress



Problem:
Energy Poverty

3+ Billion people
use less electricity than a fridge³

Solution:
More Energy



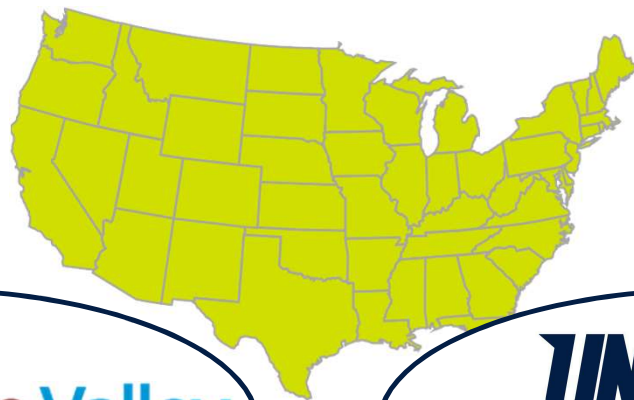
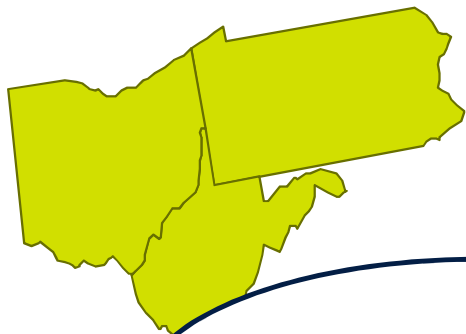
1. Source: The World Bank and The Social Progress Index as of 2015; Energy use (kg of oil equivalent per capita)
2. Source: Adapted from rogerpielkjr.blogspot.com, data sourced from The World Bank. Life Expectancy from birth (years)
3. Source: <https://www.iea.org/reports/sdg7-data-and-projections>



our Purpose:

Provide energy security for the world and lower global emissions

What we are doing

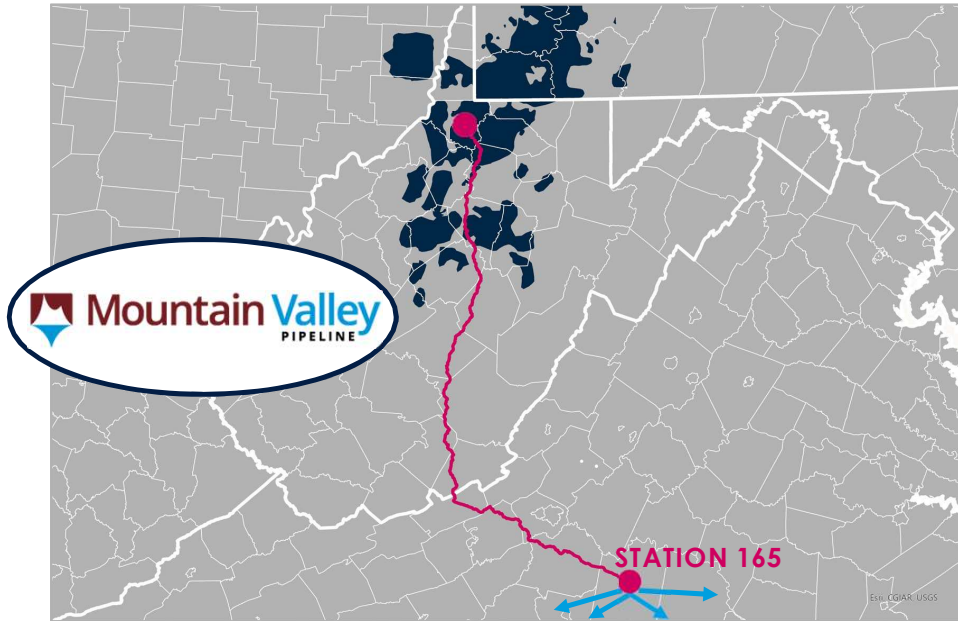


MVP Approval Highlights Bipartisan Infrastructure Support

MVP and southern expansion projects suggest growing value to EQT over time



MOUNTAIN VALLEY PIPELINE



MULTIPLE EXPANSION PROJECTS PROPOSED

MVP, along with expansion projects, should link EQT gas directly to demand growth in the SE United States, driving the potential for better price realizations & increasing FCF over time

UPCOMING STATION 165 EXPANSIONS ANTICIPATED TO MAGNIFY MVP IMPACT

PROJECT	MMBTU/D	EXPECTED IN-SERVICE
A	160,000	Winter 2024
B	78,000	Winter 2024
C	105,000	Winter 2025
D	800,000	Winter 2027
E	300,000	TBA
Total	1,443,000	

Unleashing U.S. LNG: The Largest Green Initiative on the Planet



Equal to the Combined Impact of Every Domestic Mainstream Green Solution

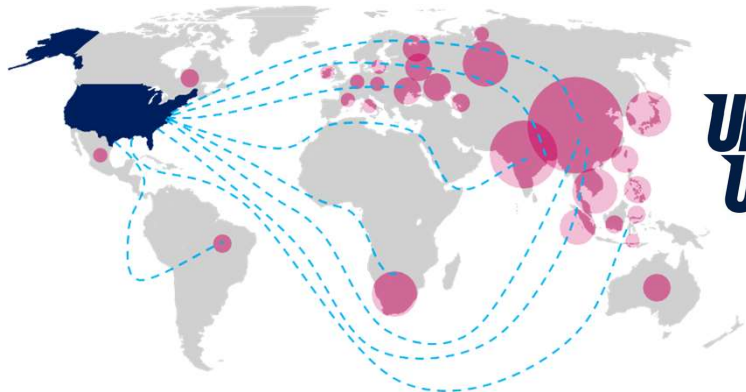
The Demand

- There is currently **175 Bcfd of coal-to-gas switching demand** in the world

The Plan

- **Quadruple U.S. LNG capacity to 55 Bcfd¹** by 2030 to replace international coal at an unprecedented pace
- Fully funded by the natural gas industry. **Ready to deploy today.**

Targeting International Coal Emissions with U.S. LNG



**UNLEASH
U.S. LNG**

The Result

- By 2030, an unleashed U.S. LNG scenario would **reduce international CO₂ emissions by an incremental -1.1 billion metric tons² per year**
- U.S. citizens will be paid for this initiative (tax revenues and an additional \$75Bn in royalties³), as opposed to paying for it

The emissions reduction impact of an unleashed U.S. LNG scenario is equal to:



Electrifying every U.S. passenger vehicle



Powering every home in America with rooftop solar and backup battery packs



Adding 54,000 industrial scale windmills, doubling U.S. wind capacity

Combined

1. Including current capacity, capacity under construction, and future new capacity 2. Assuming 3 bcf under construction, and 40 bcf additional capacity by 2030 3. Incremental cumulative royalties above 2021 levels from 2022-2030 assuming 2.0% of revenue @ \$3.75 / mcf

Source: ICCT, IEA statistics, ICF Update to the life-cycle analysis of GHG emissions for U.S. LNG exports analysis

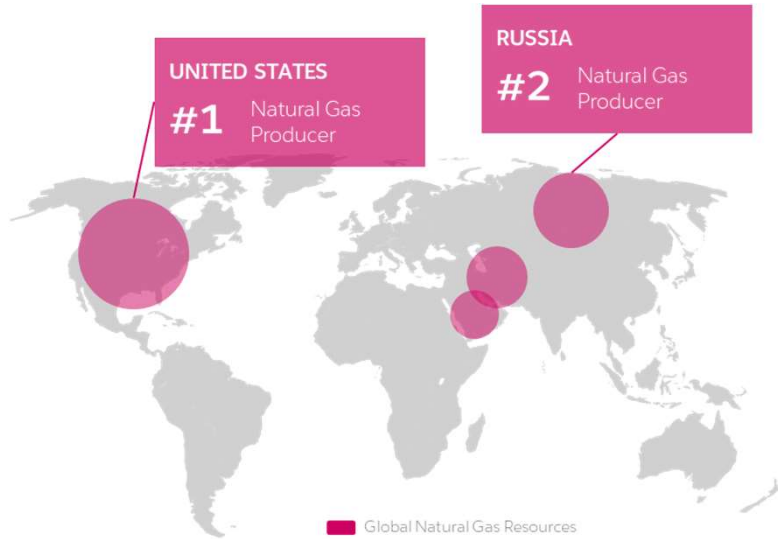
The Call for Clean, Reliable Energy Is a Call on EQT

The call on reliable, low-emissions natural gas provides exciting opportunity



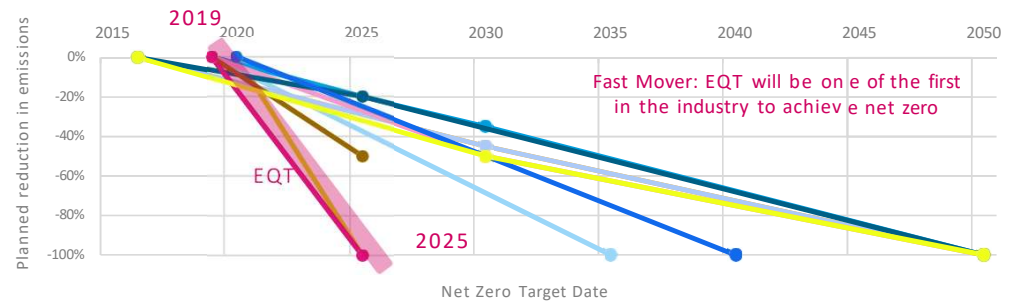
RELIABLE SUPPLY OF SCALE IS LIMITED

- ~2/3rds of the world's economically-recoverable natural gas resources are concentrated in four countries (United States, Russia, Iran and Qatar)
- **Reliable:** Direct access to the molecules of the producer from the largest resource in the free world



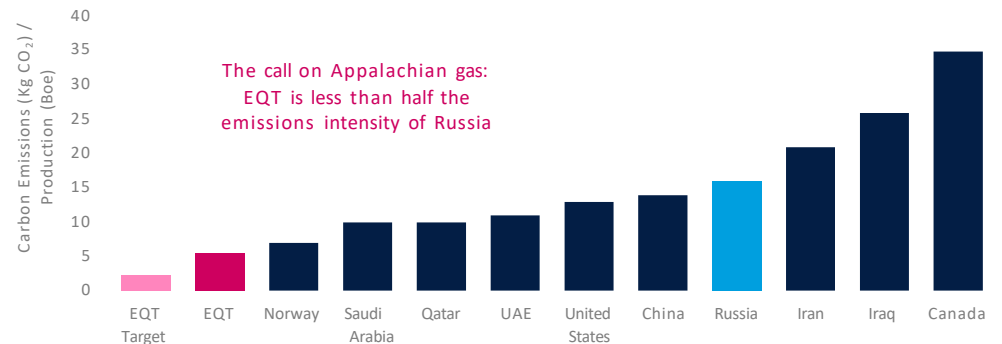
The Appalachian Basin could provide **35 Bcf/d** of incremental supply for **30-years**, the largest additional resource potential in the world

NET ZERO TARGETS⁽¹⁾ EQT vs. Peers⁽²⁾



Growing appreciation of the need for U.S. LNG to provide **energy security** to the world and play a meaningful role in addressing **climate change**

2021 EMISSIONS INTENSITY⁽²⁾



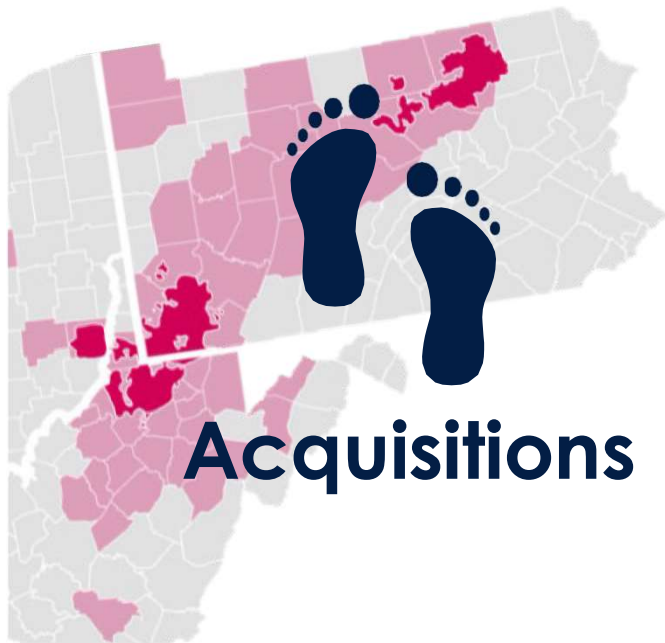
1. Companies include AR, BP, CHK, COP, CVX, DVN, HES, MRO, OXY, RDS, RRC & XOM. 2. Source: Rystad.



Our Mission:

Deliver cheaper, more reliable, cleaner energy to the world

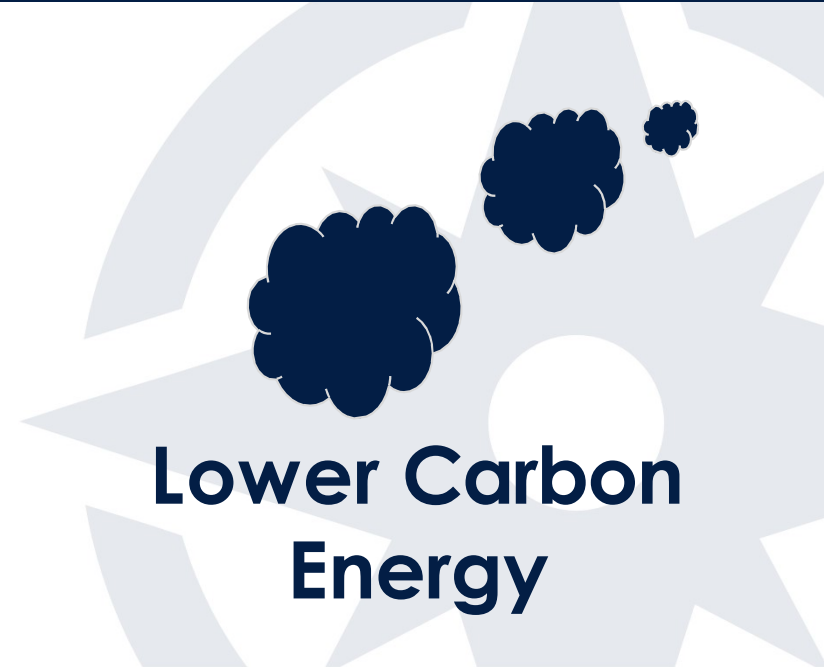
What we are doing



Acquisitions



Operational Execution

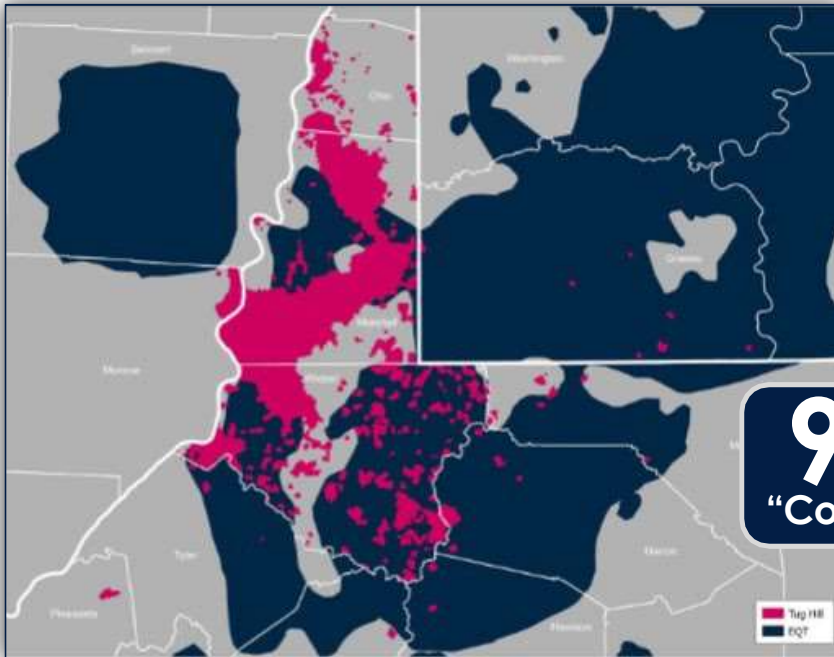


Lower Carbon Energy

EQT is doing big deals to make our energy cheaper and more reliable: Tug Hill and XcL
 Transaction closed in August, currently focused on the safe integration of these assets into our portfolio



Tug Hill: Upstream



90k
 "Core" Acres

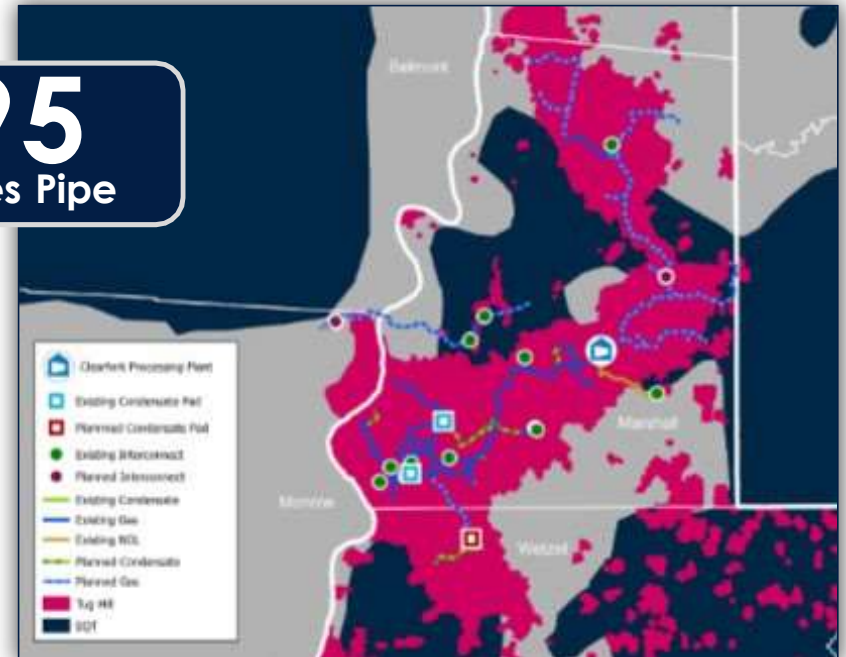
Upstream Asset Detail

300
 "Core" Net Locations

800
 Mmcfe/d

20%
 liquids

XcL: Midstream



95
 Miles Pipe

Asset Highlights

- Clearfork Processing Plant
- Existing Condensate Pad
- Planned Condensate Pad
- Existing Bifurcated
- Planned Bifurcated
- Existing Sinterment
- Planned Sinterment
- Existing Condensate
- Existing Gas
- Planned Gas
- Existing WGL
- Planned WGL
- Existing Gas
- Planned Gas
- Tug Hill
- EQT

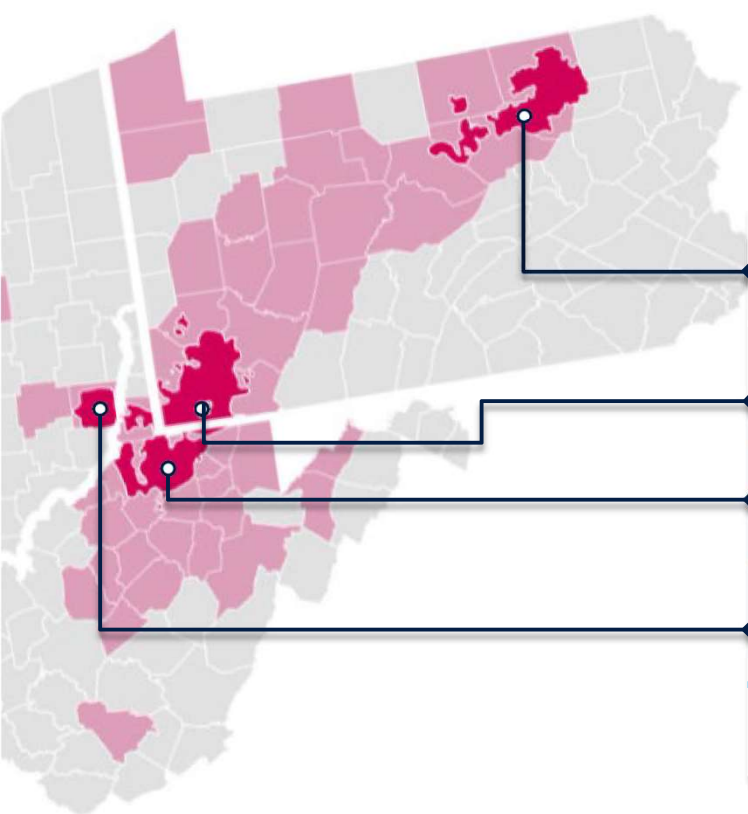
Midstream Asset Detail

4.5
 BCFD of gas pipeline capacity

225
 Mmcfd of Processing

20
 mbbls/d Cond. Processing

Appalachia is home to all operations, assets, and activity

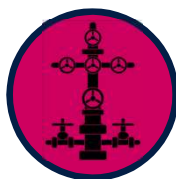


	Total Assets		2023 Activity			
	PROD FEET (Million)	PROD WELL	SITES	HZ	FRAC	SALES
NE PA	2.3	354	1	9	11	18
SW PA	11.7	1,625	5	43	62	63
WV	2.3	415	3	17	31	26
OH	1.5	142	0	0	0	0
TOTAL:	17.8	2,536	9	78	115	125

We execute large scale development programs



Existing Production



2.4 BCFD

923 HZ Wells

6,950,000 HZ feet

2023 Activity



4 New Sites



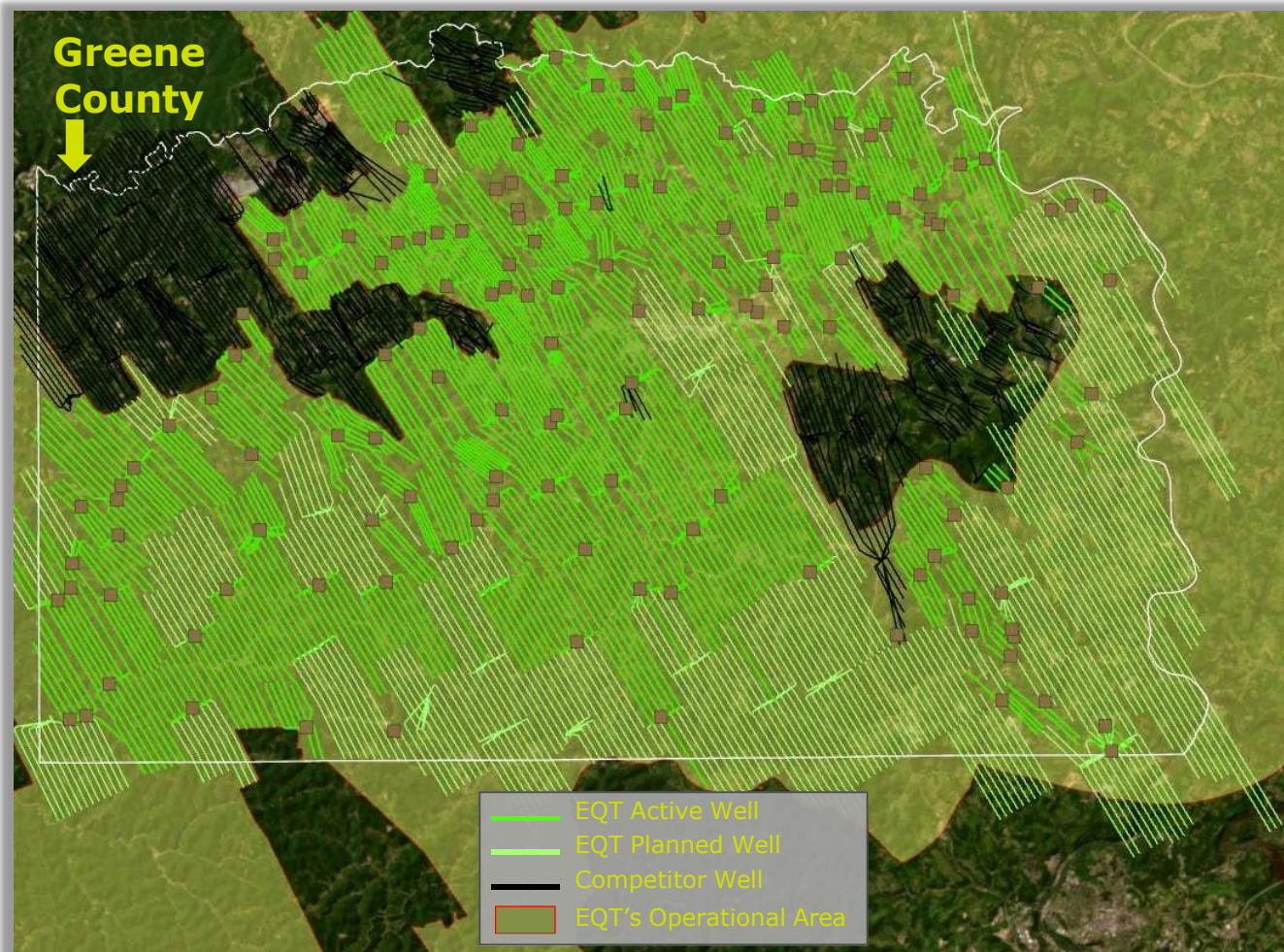
34 New Wells Drilled



59 New Wells Frac'd



63 New Wells TIL'd



EQT Drilling Efficiencies Are Pulling Ahead of Peers, Setting New Records

Performance drives peer-leading efficiencies capable of drilling 1 MM lateral feet per year with <2 rigs



SWPA & WV MARCELLUS⁽¹⁾

Drilling Faster & Further Than Peers



Avg. Spud to Total Depth Days per Rig
20% Shorter Cycle Times

7.3
days

9.2
days



Avg. Measured Depth (MD)
20% Longer Wells

21,944'
avg. MD

18,161'
avg. MD



Avg. Footage Drilled per Day
68% Faster Drilling

4,680'
per day

2,782'
per day



Avg. Equipment Move Days
48% Quicker to Next Site

3.1
days

6.0
days

575K

lateral feet drilled
per rig, annually

1.7 rigs

to drill 1 MM
lateral feet

NEW WORLD DRILLING RECORD SET

FOOTAGE DRILLED IN 48-HOURS⁽²⁾

New World
Record

18,200

Old World
Record

17,409

+5%

Old EQT
Record

16,939

**NEW EQT
DRILLING
RECORDS**

**12,318 lateral footage
drilled in 24 hours,**

> 12% increase from previous EQT record

**23,412 total footage
drilled in a single run,**

> 14% increase from previous EQT record

1. Source: Paterson UTI, 2022 – current data. 2. World record data provided by Baker Hughes.

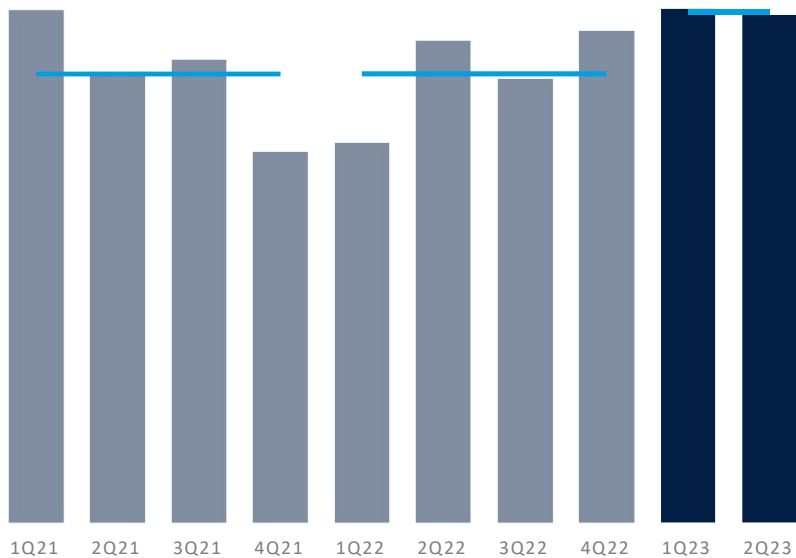
EQT Completions Program Operating at Peak Levels

New EQT record with nearly 4-mile lateral completed in Q2



AVERAGE FRAC CREW PUMPING HOURS

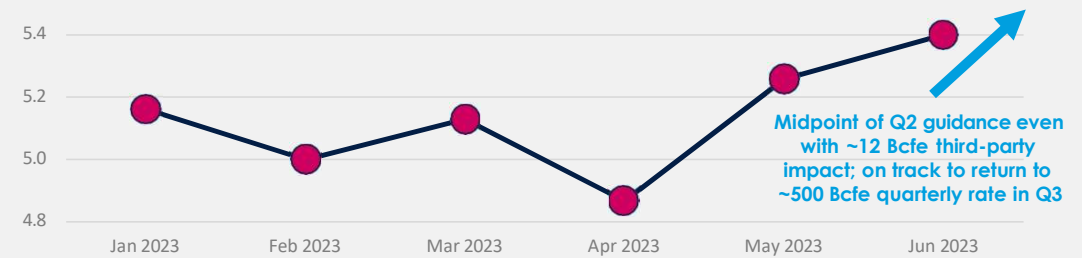
Hours



EQT COMPLETION OPERATIONS RUNNING IN-LINE WITH HISTORICAL PEAK LEVELS

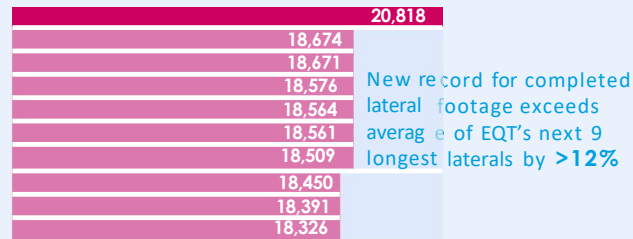
PRODUCTION RATE ON THE UPSWING

Bcfe/d

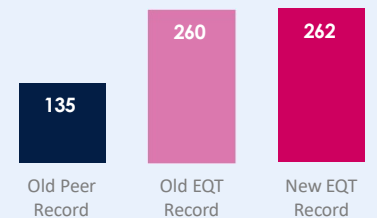


NEW COMPLETION RECORDS SET

TOP 10 EQT COMPLETED LATERAL FOOTAGE

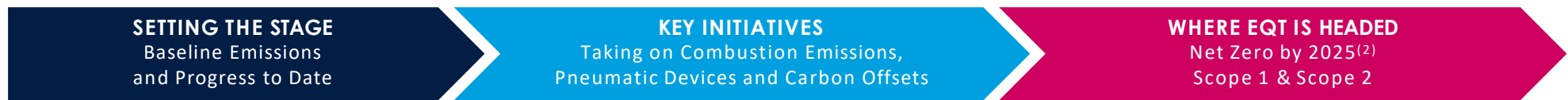


DRILLOUT PERFORMANCE # of plugs per run

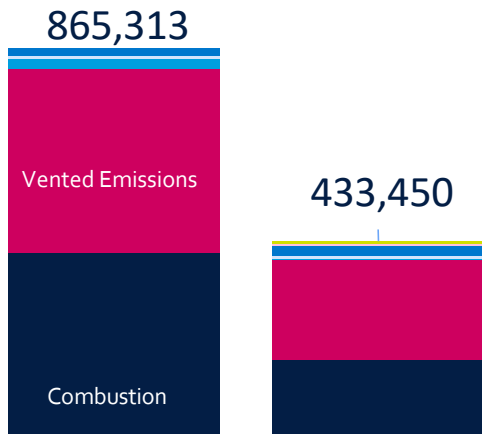


Clear Visibility Towards Achieving Net Zero Goal by 2025

Proven path to reach emissions targets, not relying on future technological advancements



Production Segment Scope 1 & 2 GHG Emissions⁽¹⁾ (MT CO₂e)



- EQT 2018 ⁽³⁾ EQT 2022
- Scope 2
 - Flared hydrocarbons
 - Process emissions
 - Completions and workover venting emissions
 - Fugitive emissions
 - Other vented emissions
 - Combustion emissions

Electrifying the Oilfield

Replaced Diesel in Completion Operations with Electric Crews

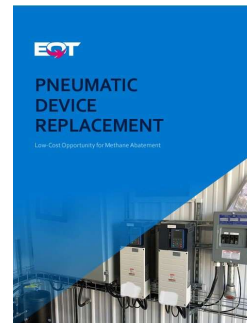


Carbon Offset Opportunities

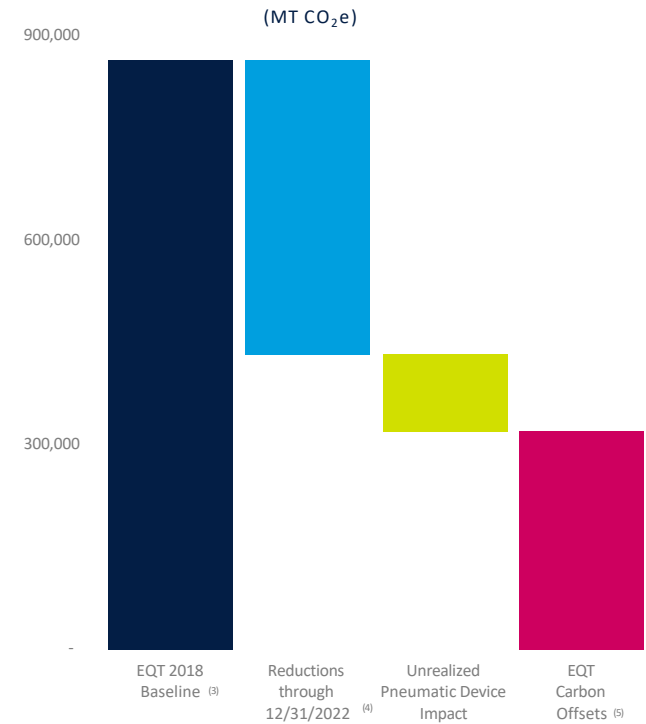
Nature-Based Carbon Offset Initiative to Offset Emissions that Cannot be Reduced with Existing Technology



Eliminated ~9,000 Natural Gas-Powered Pneumatic Devices
Leading the Industry with Published White Paper



Pathway to Net Zero^(1,2)



1. Scope 1 emissions depicts only Production segment emissions, as reported to the EPA under Subpart W; excludes emissions from the Alta Assets. 2. Net zero target is based on Scope 1 Production segment and Scope 2 GHG emissions, in each case from assets owned by EQT on June 30, 2021. 3. 2018 EQT GHG emissions data does not include Scope 2 GHG emissions, as EQT began calculating Scope 2 GHG emissions in 2020. 4. Reductions through 12/31/2022 includes impact of replacing diesel powered completions crews with electric crews and pneumatic device emission reductions realized through year-end 2022. 5. EQT-generated carbon offsets may be supplemented with purchased carbon credits.

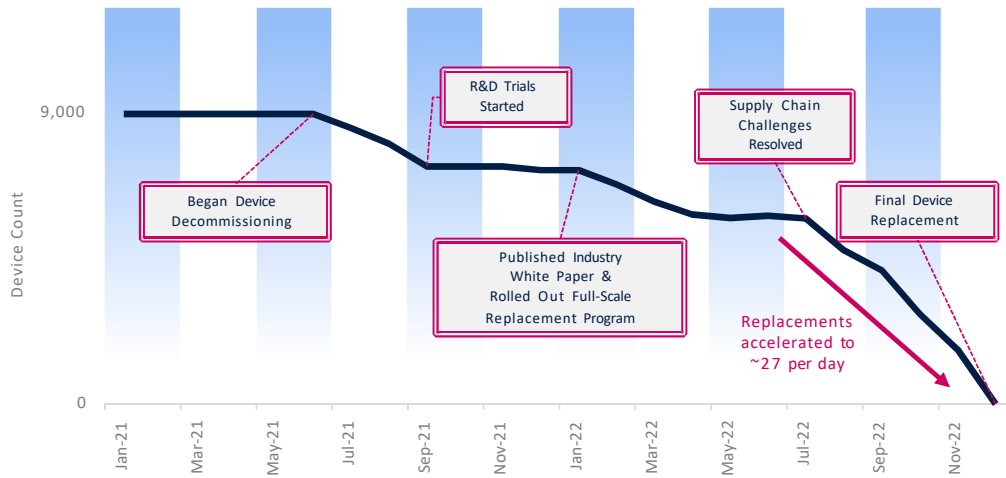
High Impact, Low-Cost Initiative Drives Down Methane Emissions

Successful elimination of natural gas-powered pneumatic devices reduces largest methane emission source



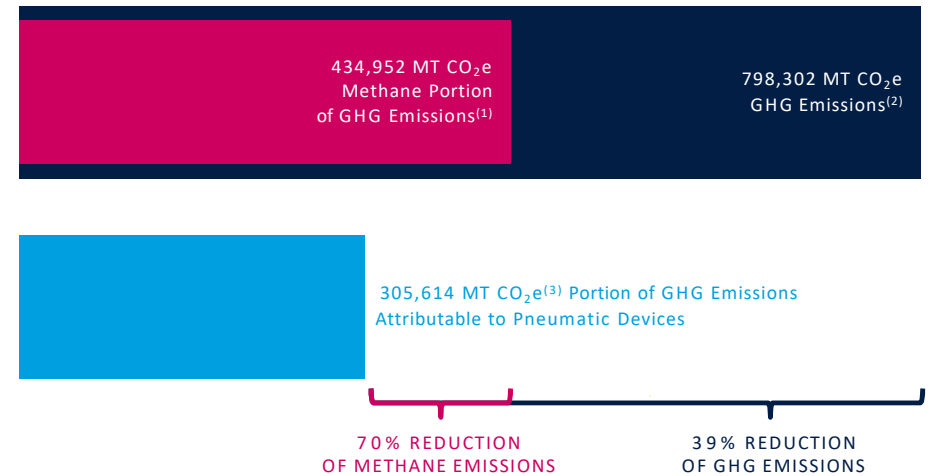
ELIMINATION OF NATURAL GAS-POWERED PNEUMATIC DEVICES COMPLETE

Replaced or retro-fitted ~9,000 devices in 18 months, 1 year ahead of schedule



2021 PRODUCTION SEGMENT SCOPE 1 EMISSIONS

Includes all assets owned at 12/31/2021



“ This milestone demonstrates our team’s exceptional ability to rapidly evolve EQT’s operations through innovation and teamwork, and better positions affordable, reliable, clean natural gas as one of the world’s most impactful decarbonizing tools. ”

- TOBY Z. RICE,
PRESIDENT & CEO

\$28 MM
Total initiative spend

~\$6/MT
of CO₂e abatement cost⁽⁴⁾

1. 2021 methane emissions for all assets owned as of 12/31/2021 converted from MT CH₄ to MT CO₂e using 100-year Global Warming Potential (GWP) for 100-year time horizon of 25. 2. Sourced from EQT ESG Performance Data published June 2022, summation of 2021 Production segment Scope 1 GHG emissions for EQT and Alta Assets. 3. Full effect of emissions reduction from pneumatic device replacements will not appear in reported emissions until calendar year 2023. 4. \$28 MM / (305,614 MT CO₂e pneumatic related emissions per year × 15 years) = ~\$6/MT of CO₂e.

Increased Transparency on EQT Progressing a Low-Carbon, Reliable Energy Future



Differentiated natural gas supply and new venture efforts support long-term goals and demand

• EQT 2022 ESG REPORT BRINGS TRANSPARENCY TO OUR PERFORMANCE

- EQT AWARDED **OGMP 2.0 GOLD STANDARD RATING**, FURTHER DIFFERENTIATING SUPPLY
- EQT HAS 3.3 BCF/D OF CERTIFIED RSG PRODUCTION, THE LARGEST PRODUCER IN NORTH AMERICA (1)
 - Natural gas certified under both the EO100™ Standard for Responsible Energy Development,

• EQT entered a strategic partnership with Context Labs

- Advances development of verified low carbon intensity natural gas products

• EQT initiated the Appalachia Methane Initiative (AMI)

- Provide methane emission monitoring across entire Appalachian basin

2022 ESG REPORT & ESG PERFORMANCE HIGHLIGHTS

NOW AVAILABLE ONLINE AT [ESG.EQT.COM](https://www.esg.eqt.com)



“EQT and Context Labs are leading the industry in capturing opportunities not just to decarbonize natural gas, but credibly validate our emissions reductions, which is a critical component to ensuring natural gas plays a leading role in the world's energy evolution.”

- TOBY Z. RICE – PRESIDENT & CEO



1. Based on the amount of North American RSG certificates issued during 2022 under MiQ's Digital Registry.

The Final Step to Zero Carbon Operations: Our First Carbon Offset Initiative

Advancing development of low carbon intensity natural gas products and verifiable carbon offsets [using nature-based solutions](#)



ANNOUNCED FIRST NATURE-BASED CARBON OFFSET INITIATIVE

PARTNERING WITH WHEELING PARK COMMISSION, TERALYTIC & CLIMATE SMART ENVIRONMENTAL CONSULTING TO GENERATE VERIFIABLE CARBON OFFSETS

- > Projects will span >1,000 acres of forest land at Oglebay, owned by Wheeling Park Commission & will utilize Teralytic's soil probe technology to ensure quantification of offsets is accurate and transparent
- > Implementing Conservation Practice Standards (CPS) outlined by U.S. Department of Agriculture's Natural Resource Conservation Service (NRCS) and will align to Verra guidelines to ensure effectiveness of emissions reductions
- > EQT also partnered with Wheeling Country Day School to pilot educational program to allow students to learn about soil health by monitoring real-time changes in the health of the soil, 24 hours a day



“Nature-based projects like this, which are supported by cutting edge technology that ensures accuracy and transparency, will help offset EQT's remaining emissions and advance our mission to deliver cheaper, more reliable, cleaner energy to the world.”

- ROB WINGO – EVP, CORPORATE VENTURES



What's after Net-Zero? Appalachian Regional Clean Hydrogen Hub (ARCH2)



EQT's natural gas will be used as feedstock to enable and sustain a regional H2 economy

Purpose

ARCH2 will use our region's natural gas to enable and sustain a regional H2 economy across multiple end-use sectors while ensuring economic benefits for our communities

Projects

Projects cover entire blue and green H2 value chain including production, liquefaction, storage and transportation, offtake, fueling and blending

Total Investment

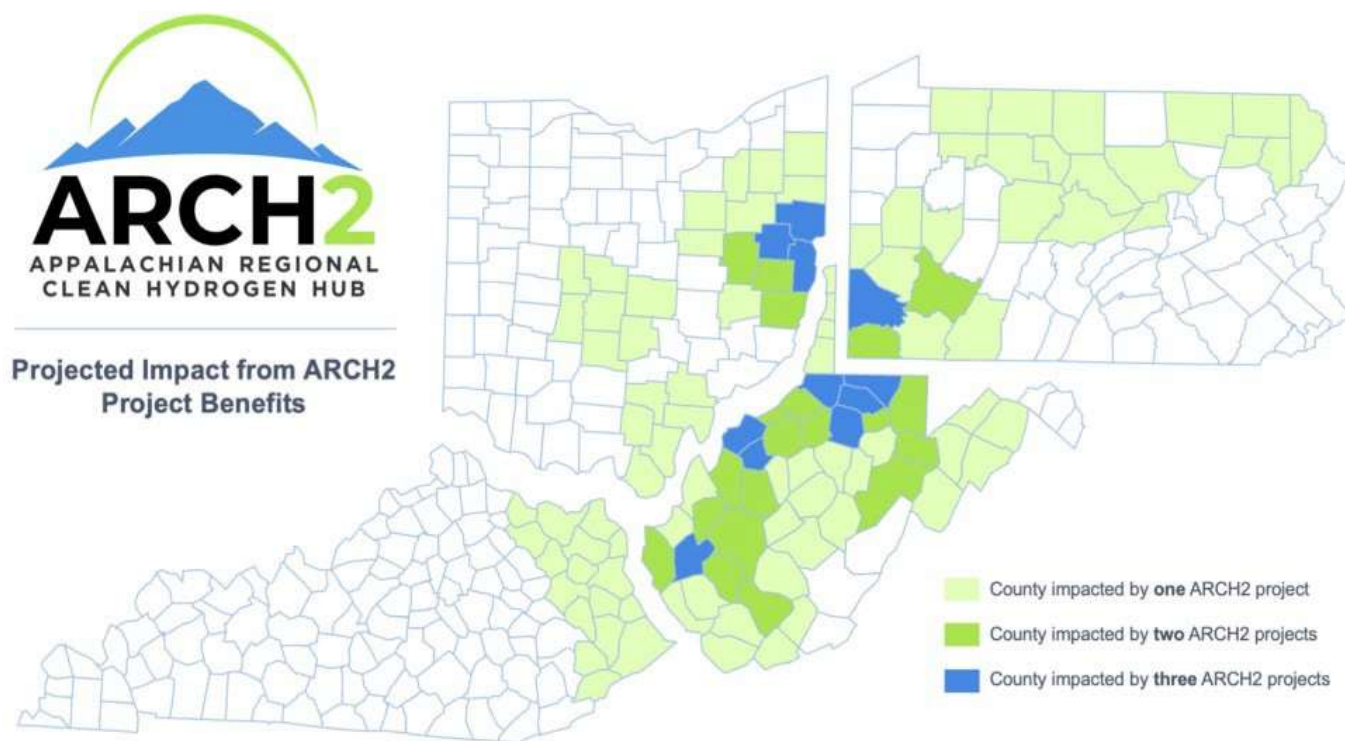
~\$6 billion

Timing

- Expected DOE selection for FID approval by late '24/early '25
- Kick-off in '25 and in service by '28

Competition

Approximately 30 hub teams are competing, but the DOE will only select 8 to 12 hub winners to proceed



ARCH2: Partners in Growth + Energy Transition

Attracting growth and investment in Appalachia from new and existing community partners



PROGRAM MANAGEMENT AND TECHNICAL SUPPORT

BATTELLE  **GTI ENERGY**  **AST**
Allegheny Science & Technology  **TRC**  **NETL** NATIONAL ENERGY TECHNOLOGY LABORATORY

PROJECT DEVELOPERS

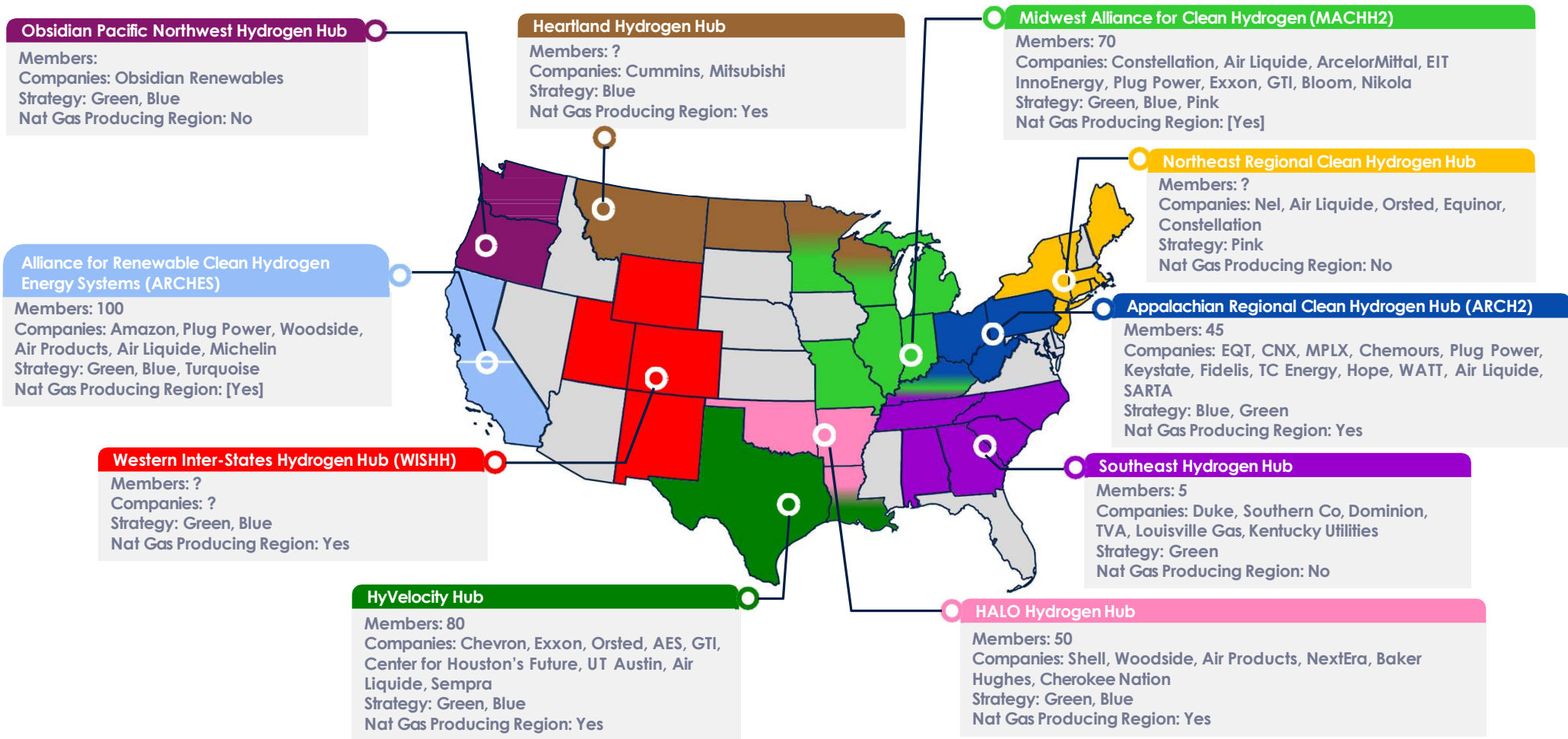
 **Air Liquide**  **CNX**™  **Clearway Energy**  **Dominion Energy**™  **EMPIRE**
Diversified Energy

 **EQT**  **FIDELIS**
NEW ENERGY  **HOG LICK**
AGGREGATES  **Hope Gas**  **IH**
Independence Hydrogen

 **FIRST MODE**  **KeyState Energy**  **MPLX**  **TC Energy**  **plug**™

Top hub competitors

Leaders have surfaced in the highly competitive landscape for DOE's Regional Clean Hydrogen Hubs program





Our Vision:

Become the operator of choice for all stakeholders

What we are doing



**Community
Engagement**



**Community
Giving**



Community Engagement

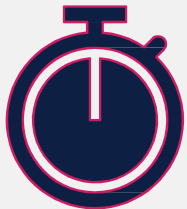
In the past year:



- 28,500 calls
- 23,000 emails



30,000
cases resolved



7 days
average resolution time

Our landowners are our valued partners



HOW TO **CONTACT US:**

- **Call: 844-EQT-LAND**
– Available Mon-Fri from 8AM-4:30 PM EST
- **Email: OwnerRelations@eqt.com**
- **Website: www.eqt.com/contact**
- **Mail:** EQT Production Company
Attention: Owner Relations
400 Woodcliff Drive
Canonsburg PA 15317

Our Owner Relations Qrew is here to help serve the needs of our landowners

Community Giving

EQT is an active community partner throughout our operational footprint



2022 Giving Summary



14,000+
volunteer hours



\$41+ Million
Dollars Invested

