Oil and Gas, Natural Resources, and Energy Journal

Volume 2 | Number 6

March 2017

Terrorism and Oil & Gas Pipeline Infrastructure: Vulnerability and Potential Liability for Cybersecurity Attacks

Joseph R. Dancy

Victoria A. Dancy

ONE J

Oil and Gas, Natural Resources, and Energy Journal

VOLUME 2 NUMBER 6

TERRORISM AND OIL & GAS PIPELINE INFRASTRUCTURE: VULNERABILITY AND POTENTIAL LIABILITY FOR CYBERSECURITY ATTACKS

JOSEPH R. DANCY & VICTORIA A. DANCY*

Table of Contents

* Joseph R. Dancy is the Interim Director of the University of Oklahoma College of Law Oil and Gas, Natural Resources, and Energy Center and is an Adjunct Professor at SMU Dedman School of Law and SMU Cox School of Business. He graduated from Michigan Technological University with a B.S. in Metallurgical Engineering/Mineral Processing before earning an MBA at the University of Michigan and a JD from Oklahoma City University School of Law. He is also president of LSGI Advisors Inc., a research and investment firm headquartered in Dallas and is a Texas Representative to the Interstate Oil & Gas Commission.

Victoria A Dancy is Deputy Regional Counsel of the Federal Deposit Insurance Corporation, Dallas Regional Office, graduating from the University of Idaho with a B.S. in Mining Engineering before earning an MBA and a JD from Oklahoma City University. She was in private practice before joining the FDIC where she has participated in several hundred institution failures preparing resolution documents and serving as on-site lead closing attorney.

A special thanks to University of North Texas College of Law students Rachel Hawkins, Matthew Sayegh and Raul Mijares for their research assistance.

I. Executive Summary

Crude oil and natural gas production in the U.S. has dramatically increased with the recent technological advances in drilling and completion techniques. This production is processed, transported, distributed, and sold via an extensive North American pipeline network.

Roughly two-thirds of U.S. energy demand is transported by pipeline. Due to a number of factors discussed in this paper this delivery system is quite vulnerable. Under the current regulatory structure there are few mandated standards regarding pipeline cybersecurity. Regulators rely on voluntary standards adopted by state and federal agencies, developed with industry assistance.

Despite being more important to national commerce than ever, numerous existing pipeline systems are quite dated. Many utilize outdated technology and were constructed utilizing techniques and materials prone to excessive rates of failure due to latent construction and material defects.

Statistical analysis indicates pipelines more than forty years old are much more likely to rupture or leak under standard operating conditions. Meanwhile, most pipeline systems have become more automated and, in theory, have also become increasingly more vulnerable to data breaches and cyber intrusions. While there have been no major incidents involving a domestic cyberattack on the pipeline infrastructure, the risks are increasing exponentially. A major cyberattack on energy infrastructure would not be unexpected under the current regime and, if carried out, would result in a potentially devastating circumstance.

In this analysis, we examine the current state of the pipeline infrastructure in the U.S., the potential physical and cyber threats to such systems, the issue of whether voluntary cybersecurity standards are sufficient to protect the public from harm, as well as potential tort liability for cyber intrusions and the associated legal issues.

II. Introduction

Cybersecurity issues have become a major concern of many domestic consumer, financial, industrial, and retail organizations.[1] With the general public devoting most of its attention to the cyber intrusions within these organizations, few realize that the energy sector—including pipelines, power plants, refineries, transmission grids, and even individual wells—are potentially a major target for cyberattacks or intrusion.[2] According to the Department of Homeland Security the energy sector has incurred more cybersecurity incidents than any other sector over the past several years.[3]

A November 2015 survey issued by security vendor Tripwire indicated that 82% of oil and gas industry respondents reported their organizations experienced an increase in cyberattacks over the previous 12 months.[4] Additionally, 53% of respondents stated that the rate of cyberattacks had increased between 50% and 100% during that same period.[5] The survey noted further that almost seven out of ten respondents indicated a lack of confidence in their organizations to detect and stop attacks.

Potentially, these intrusions could result in millions of dollars in economic damages or drastic harm to the environment, all while putting the welfare and safety of U.S. citizens at risk. With the possibility of cyberattacks looming, the oil and gas industry has become aware of the

---

1. *See* Noah G. Susskind, Note, *Cybersecurity Compliance and Risk Management Strategies: What Directors, Officer, and Managers Need to Know*, 11 N.Y.U. J.L. & Bus. 573 (2015).

2. *See* Michael L. Krancer et al., *Energy Sector Beware: Cybersecurity Now Top Security Threat*, The Legal Intelligencer, Oct. 16, 2015, http://www.thelegal intelligencer.com/id=1202739941630/Energy-Sector-Beware-Cybersecurity-Now-Top-Security-Threat?mcode=0&curindex=0&curpage=ALL.

3. *Id*.

4. *In the Pipeline*, Insurance Business, Aug. 18, 2016, http://www.ibamag.com/news/cyber/in-the-pipeline-36549.aspx.

5. *Id*.; *See, e.g.*, *Cyber Attacks Hit Oil, Gas, Just as Much as Retail*,Greeley Tribune, Apr. 1, 2014, where it was noted the Director of the National Security Agency and head of the U.S. Cyber Command stated that energy companies were targeted in 41% of the malicious software attack cases reported to the Department of Homeland Security in 2012.

growing threat and its vulnerability. In a 2015 survey, Ernst & Young reported that "61% of oil and gas organizations surveyed believed they would be unlikely to be able to detect and react to a sophisticated cyberattack."[6]

A recent *Wall Street Journal* survey of information technology executives in both the U.S. and in Europe found that 48% believed it is "likely there will be a cyberattack on critical infrastructure in the next three years that will result in the loss of life."[7] These surveys also note the cost of cybersecurity threats, with the assets required to address these threats increasing at an alarming rate.

This cybersecurity threat extends across the energy sector, from oil and natural gas wells, pipelines, processing plants, refineries, gas utilities, to hydrocarbon retailers.[8] In this analysis we will focus on the state of the nation's liquid and natural gas pipeline system, its vulnerability to cyberattacks, and the potential liability of pipeline operators.

Cybersecurity threats to pipeline operations are increasing in importance as the volume of crude oil and natural gas production in North American is increasing and, after production, these substances are being shipped further distances to market.[9]

Advances in drilling and hydraulic fracturing technology have increased crude oil production in the U.S. by roughly 72% and natural gas by 30% from 2010 to 2015, according to U.S. Energy Information Administration data.[10] Numerous new pipelines are being built or expanded to handle the

---

6. Jon Mainwaring, *Five Jobs Set to Grow in Oil, Gas: Cybersecurity*, Rigzone (May 3, 2016), http://www.rigzone.com/news/oil_gas/a/144291/five_jobs_set_to_grow_in_oil_gas_cybersecurity (citing PwC Inc. survey findings that security incidents detected by oil and gas firms increased by 93% in the previous year.).

7. Ben Dipietro, *Survey Roundup: Deadly Cyberattack Worries*, Wall St. J. (Jul. 24, 2015), http://on.wsj.com/1CVsrWK (notably "critical infrastructures" included but was not limited to pipelines after surveying 625 IT professionals).

8. *See, e.g.*, Elisabeth R. Myers, *Oil Pipelines*, 2010 A.B.A. Recent Dev. Pub. Util. Comm. & Transp. 16 (2010), *available at* http://www.huschblackwell.com/~/media/files/businessinsights/businessinsights/2010/07/oil%20pipelines%202010%20edition%20of%20emrecent%20developme__/files/100720_oilpipelines/fileattachment/100720_oilpipelines.pdf.

9. *See* Pierre Bertrand, *Ensuring Pipeline Physical and Cyber Security*, Plant Engineering (May 20, 2015), http://www.plantengineering.com/single-article/ensuring-pipeline-physical-and-cyber-security/a0f2373b0adc20ac7cc40aef5a52b2a8.html.

10. *See* U.S. Energy Information Administration, *Petroleum & Other Liquids*, database at https://www.eia.gov/dnav/pet/pet_crd_crpdn_adc_mbblpd_a.htm; see also U.S. Energy Information Administration, *U.S. Dry Gas Production*, database at https://www.eia.gov/dnav/ng/hist/n9070us2M.htm.

additional volumes of hydrocarbon volumes being transported across North America.[11]

It is estimated that the U.S. currently has 182,000 miles of hazardous liquid pipelines,[12] 325,000 miles of natural gas transmission pipelines, and 2.15 million miles of natural gas distribution pipelines along with the associated metering, pumping, sensors, and valves that accompany each.[13] Over 3,000 private and public companies own and operate the nation's pipelines according to recent estimates.[14] Due to the ubiquitous nature of the energy delivery system a cyberattack on such energy infrastructure presents the risk of "unfathomable asymmetrical physical damage" to life and property according to some experts.[15]

Those who study cybersecurity issues realize that it is potential cyberattacks on the energy space, not the consumer credit space, that could cripple the United States economy.[16] At the extreme end of the spectrum a large cyberattack on energy infrastructure could bring about a collapse of society that most of us associate with apocalyptical scenarios.

The costs of such a pipeline system cybersecurity breach include the cost of business interruption, damage to third parties, and damage to the physical plant or equipment and control systems. For those companies that are publicly traded, the cost could include a large post-breach drop in the

---

11. Sabine Hoover, *Energy Outlook: Key Trends Impacting the Construction Industry*, Construction Executive (Jan. 15, 2015), http://enewsletters.constructionexec.com/managingyourbusiness/2015/01/energy-outlook-key-trends-impacting-the-construction-industry/; *see also P&GJ's 2017 Worldwide Pipeline Construction Report*, Pipeline & Gas Journal. (Jan. 2017), https://pgjonline.com/2017/01/03/pgjs-2017-worldwide-pipeline-construction-report/ (noting that North America leads the world in pipeline construction with 31,814 miles of new or planned lines for oil and natural gas).

12. Hazardous liquids pipelines include pipelines transporting crude oil, natural gas liquids, gasoline, and other petroleum hydrocarbons.

13. *See* Belle Hillenburg, *Nation's Pipeline Increasingly at Risk of Cyber, Physical Attacks*, HOMELAND SECURITY TODAY, (May 9, 2016, 6:00 AM), http://www.hstoday.us/single-article/nation-s-pipelines-increasingly-at-risk-of-cyber-physical-attacks/e55550d405dcb 5ba3f1 e9ca1cabc7757.html.

14. *Pipelines: Securing the Veins of the American Economy*: *Hearing Before the H. Subcomm. on Transp. Sec.*, 114th Cong. 1 (2016) (statement of Sonya Proctor, Surface Division Director, Office of Security Policy and Industry Engagement), *available at* http://docs.house.gov/meetings/HM/HM07/20160419/104773/HHRG-114-HM07-Wstate-ProctorS-20160419.pdf.

15. Krancer et al., *supra* note 2.

16. *See, e.g.*, Michael Krancer, *The Biggest Cybersecurity Threat: The Energy Sector*, Forbes (Nov. 4, 2015), https://www.forbes.com/sites/michaelkrancer/2015/11/04/the-biggest-cybersecurity-threat-the-energy-sector/#6fbe128 736ba.

stock value.[17] For example, past post-breach market reaction has led to declines in shareholder values ranging from 17% to over 30% as well as creating business and market disruptions that can last for weeks.[18] Due to the limited extent of disclosures required for a cybersecurity breach, damages are difficult to estimate. Some analysts, however, claim oil and gas companies lose $8.4 million per day due to cyberattacks.[19]

Both applicable regulations and tort laws are evolving as cyber intrusions become more commonplace. In many cases, the industry along with federal and state regulators face issues and fact scenarios regarding cyber intrusions that have never been addressed – an exciting frontier in the energy sector where courts and regulatory agencies have already meticulously addressed most other exploration issues.

III. SCADA Data Systems

As with many industries, the energy sector has become more and more reliant on computerized control and data systems. Among the more commonly utilized operational control systems employed in the energy sector are the Supervisory Control and Data Acquisition ("SCADA") systems.[20]

SCADA systems are software-based control systems that can monitor and control multiple aspects of operations for a variety of industrial and utility sectors including railways, utility power grids, water and sewer systems, and pipeline networks.[21]

SCADA systems can collect real-time data such as line pressure from sensors located throughout the pipeline network. This data can be monitored by operators from a remote control room, often many miles away from the physical operations.[22] SCADA systems provide the operator with

17. *See* Susskind, *supra* note 1, at 575.

18. *Id.*

19. Hillary Hellmann, Comment, *Acknowledging the Threat: Securing United States Pipeline SCADA Systems*, 36 Energy L.J. 157, 158 (2015) (citing Stewart Baker et al., *In the Dark: Critical Industries Confront Cyberattacks*, McAfee (2011)).

20. *See, e.g.*, Hellmann, *supra* note 19; *see also CAE, Inc. v. Clean Air Eng'n Inc.*, No. 97 C 3264, 2000 WL 28274, at *3-4 (N.D. Ill. Jan. 10, 2000), *aff'd*, 267 F.3d 660 (7th Cir. 2001).

21. *See, e.g.*, PAUL W. PARFOMAK, CONG. RESEARCH SERV., R42660, PIPELINE CYBERSECURITY: FEDERAL POLICY 3 (2012), http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-076.pdf; *see also Clean Air Eng'n*, 2000 WL 28274, at *3-4 (Jan. 10, 2000).

22. *See* PARFOMAK, *supra* note 21, at 3*; see also* Hellmann, *supra* note 19, at 159.

feedback and information about the entire pipeline system and triggers safety alarms when operating conditions are not within the prescribed design parameters.[23] For example SCADA systems monitor pressures, temperatures, tank levels, pump speeds among other variables.

As the court noted in *Clean Air Engineering*, SCADA systems can "reduce operating costs by optimizing system efficiency and maximizing resource utilization. These features enable companies to study and evaluate their processes and to improve efficiency and safety in critical situations."[24]

Operators can send commands from their SCADA workstations to control the pipeline infrastructure, which includes valves, pumps, and compressor stations.[25] While this technology is integral to the functionality of modern day pipeline systems, SCADA systems have become increasingly vulnerable to outside invasion and manipulation.[26]

The Congressional Research Service recently released a summary on pipeline security, concluding the domestic network is "increasingly vulnerable" to cyberattacks.[27] Specifically, the report notes that "cyber infiltration of [SCADA] systems could allow successful 'hackers' to disrupt pipeline services and cause spills, explosions, or fires—all from remote locations via the Internet or other communication pathways."[28]

SCADA-related problems were identified to be part of, if not the proximate cause of recent pipeline accidents, some of which resulted in extreme consequences.[29] For example, in what has been commonly known as the "San Bruno pipeline explosion," a 30-inch diameter natural gas transmission pipeline owned and operated by PG&E ruptured and caught

---

23. Trudy E. Bell, *Pipeline Safety & Security: Is It No More Than a Pipe Dream?*, The Bent, at 13, 15 (2015), http://www.tbp.org/pubs/Features/W15Bell.pdf (identifying that it is not uncommon for operators to not respond to alarms o the SCADA systems due to the number of false alarms).

24. *Clean Air Engin'n*, 2000 WL 28274, at * 3 (Jan. 10, 2000).

25. *See id.* at 3-4; *see also:* Hellmann, *supra* note 19, at 159-60.

26. *See* Hellman, *supra* 19, at 160-65.; *see also Pipelines: Securing the Veins of the American Economy*: *Hearing Before the H. Subcomm. on Transp. Sec.*, 114th Cong. 4 (2016) [hereinafter Parfomak Testimony] (statement of Paul W. Parfomak, Specialist in Energy and Infrastructure Policy), http://docs.house.gov/meetings/HM/HM07/20160419/104773/HHRG-114-HM07-Bio-ParfomakP-20160419.pdf ("The increased vulnerability of pipeline SCADA systems due to their modernization, taken together with the emergence of SCADA-specific malicious software and the recent cyber attacks, suggests that cybersecurity threats to pipelines have been increasing.").

27. *See* PARFOMAK, *supra* note 21, at 9.

28. *Id.* at 1.

29. *Id.* at 4.

fire in San Bruno, California due to "erroneous and unavailable SCADA pressure readings."[30] Gas escaping from the rupture ignited, resulting in the loss of 8 lives, injuries to 58 people, destruction of 38 homes, moderate to severe damage to 17 homes, and minor damage to 53 homes.[31] Further illustrative, in June 1999, an oil pipeline in Bellingham, Washington, ruptured due to the faulty use of the SCADA system, spilling 237,000 gallons of gasoline into a creek. The gasoline ignited, killing three, injuring eight, and causing $45 million in damage.[32] Others have noted that a 2005 refinery explosion in Texas City, Texas, resulting in the death of 15 people and the injury of 170 others, was due in part to faulty SCADA signals.[33]

In the extensive investigation following the San Bruno pipeline explosion, California regulators found "deficiencies in PG&E's SCADA system" – despite the fact that it was one of the largest and most sophisticated in the nation – in addition to inadequate controls in place at the district center responsible for emergency response.[34] While the incidents were accidental, they demonstrate the damage that can occur from a pipeline system being breached by a third-party's cyberattack.

A recent report from the Congressional Research Service concluded that the modernization of SCADA systems, the emergence of SCADA-specific malicious software, and recent attempted cyberattacks point to the conclusion that cybersecurity threats to domestic pipelines are increasing to what some might describe as an alarming level.[35]

---

30. *See id.* at 4; *see also Pac. Gas & Elec. Co. v. Pub. Utilities Comm'n*, 237 Cal. App. 4th 812, 823 (2015) (noting the Commission's consumer protection and safety division concluded that there were deficiencies in pipeline construction and a failure to follow industry practices among other problems.).

31. *Id.* at 821.

32. *See* PARFOMAK, *supra* note 21, at 4; *see also* JOSEPH WEISS, PROTECTING INDUSTRIAL CONTROL SYSTEMS FROM ELECTRONIC THREATS 123-28 (2010).

33. *See SCADA Systems and the Terrorist Threat: Protecting the Nation's Critical Control Systems: Hearing Before the H. Subcomm. on Economic Security, Infrastructure Protection, and Cybersecurity*, 109th Cong. 84 (2005), *available at* https://fas.org/irp/congress/2005hr/scada.pdf ("This accident did not involve a cyber attack, but the accident evolved as a result of the misinterpretation of signals and indicators, which could be affected by a cyber attack.").

34. *Pac. Gas & Elec. Co.*, 237 Cal. App. 4th at 823 (PG&E's SCADA system was called "*one of the largest in the U.S., providing remote control of 6,438 miles of transmission pipeline" (Id.* at note 4) (emphasis added)).

35. PAUL W. PARFOMAK, CONG. RESEARCH SERV., R41536, KEEPING AMERICA'S PIPELINES SAFE AND SECURE: KEY ISSUES FOR CONGRESS 5 (2013), https://www.aga.org/sites/default/files/pipeline_security_crs_march_2012.pdf.

Cyber intrusions into SCADA control systems for oil and gas wells and gathering systems have already caused potential environmental as well as physical equipment damage. For example, in *Vaquero Energy, Inc. v. Herda*[36] an operator of oil and gas wells, treating equipment, and pipeline gathering systems in Texas, Colorado, California, and Wyoming hired a third-party vendor to maintain and upgrade their SCADA control system's software and hardware.

The third-party vendor altered the SCADA software in such a manner the operator could not access the computer system to monitor and control the wells, gathering lines, treating, storage and pipeline equipment.[37] As a result, an oil treater overheated and was damaged. In addition, overflow and process alarms had been disabled.[38] This lack of operating alarms put the employees at danger and potentially could have caused the oil, gas, and saline produced water to have been released, harming both the environment and third parties in the immediate vicinity.[39]

The natural gas in *Vaquero Energy* contained hydrogen sulfide, otherwise known as "sour gas," which can be deadly to humans and animals if inhaled even in small quantities. The court issued an injunction preventing the third-party contractor from keeping the operator from accessing the SCADA control system, noting "environmental injury, by its nature, can seldom be adequately remedied by money damages and is often permanent or at least of long duration, i.e., irreparable."[40]

A. Infrastructure Cyberattacks

While physical attacks on pipelines have been more common, cyberattacks on pipeline systems are becoming more frequent as systems are computerized. For example, in June 1982, a major explosion occurred on the Trans-Siberian gas pipeline. The pipeline's control software unknowingly contained malicious code that massively increased the pipeline pressure, eventually leading to the explosion.[41]

---

36. No. 1:15-CV-0967-JLT, 2015 WL 5173535 (E.D. Cal. Sept. 3, 2015).

37. *Id.* at *12.

38. *Id.* at *6, 9.

39. *Id.* at *8 (An employee of the operator claimed the intrusion could cause "a H2S gas release, high pressure steam release, fire, oil spill, or pipeline rupture.").

40. *Id.* at *13 (quoting *Amoco Prod. Co. v. Village of Gambell*, 480 U.S. 531, 545, (1987)).

41. *See* Eric. J. Byres, *Cyber Security and the Pipeline Control System*, Pipeline & Gas Journal, Feb. 2009, *available at* https://pgjonline.com/2009/03/20/cyber-security-and-the-pipeline-control-system/.

One account of the incident noted "the pipeline software that was to run the pumps, turbines, and values was programmed to go haywire, after a decent interval, to reset pumps speed and value settings to produce pressures far beyond those acceptable for pipeline joints and welds."[42] The resulting three-kiloton explosion was the equivalent of a nuclear weapon, one of the largest non-nuclear explosions in history, disrupting gas supplies and Russian exports for over a year.[43]

In the winter of 2002-2003, hackers possibly affiliated with an oil industry strike penetrated a SCADA system of Petroleos de Venezuela, S.A. that was responsible for crude oil tanker loading for international export. The hackers erased programmable logic controllers in storage and pipeline systems which delayed crude oil loading.[44]

More recently, the 1,099-mile-long Baku-Tbilisi-Ceyhan ("BTC") pipeline was outfitted with both sensors and cameras to monitor every inch of the line from the Caspian Sea to the Mediterranean Sea. Traversing strategic, politically unsettled terrain, the forty-inch diameter line was built to be one of the most secure in the world.[45] But when the pipeline exploded in 2008, it was a mystery why no alarm systems were triggered and why monitoring cameras failed to pick up any unusual activity. Over 30,000 barrels of oil spilled after the pipeline exploded and caught fire.[46]

Only years later did authorities discover the BTC pipeline explosion was, in fact, the result of a sophisticated cyberattack on the pipeline's control system.[47] The hackers entry point into the control system was, ironically, through the pipeline's surveillance camera system.[48] The incident cost more

---

42. *Id*. (quoting THOMAS REED, AT THE ABYSS: AN INSIDER'S VIEW OF THE COLD WAR 269 (Presidio Press 2005)).

43. *See* Alec Russell, *CIA plot led to huge blast in Siberian gas pipeline*, The Telegraph (Feb. 28, 2004), http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html; *see also* William Safire, *The Farewell Dossier*, N.Y. Times (Feb 2, 2004) (U.S. intelligence agencies initially thought that the blast could have been a small nuclear device detonated by the Russians, raising security concerns.).

44. *See* Byres, *supra* note 41.

45. *See* Jordan Robertson & Michael Riley, *Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar*, Bloomberg (Dec. 10, 2014), https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar; *see also* Parfomak Testimony, *supra* note 26, at 2.

46. *See* Robertson & Riley, *supra* note 45.

47. *Id.*

48. *See id.*; *see also* Graham Speake, *Cybersecurity 2015: Connected Pipelines and Proliferation of Threats to Infrastructure*, Pipeline & Gas Journal (May 2015),

than $5 million per day in lost transport tariffs and the State Oil Fund of the Republic of Azerbaijan lost nearly $1 billion in export revenue.[49]

Domestically, in 2012, the Industrial Control Systems Cyber Emergency Response Team ("ICSCERT") within the Department of Homeland Security ("DHS") became aware of a identified a continual series of attempted cyberattacks against U.S. natural gas pipeline operators that had begun in December 2011.[50] ICSCERT reported that various pipeline companies experienced targeted "spear-phishing" attempts and invasions into many natural gas pipeline organizations, all possibly related to a single campaign to disrupt pipeline operations.[51]

B. Physical Attacks

Physical attacks on pipelines and pipeline systems using explosives or other means have exposed the potential vulnerability and damage that could occur should they rupture or otherwise fail.[52] As the following examples illustrate, pipeline systems have long been the target of numerous plots intended to cause significant damage. In 2005, a U.S. citizen sought to conspire with Al Qaeda to attack a major natural gas pipeline in the eastern region of the United States.[53] In 2006, federal authorities discovered a posting on a website purportedly linked to Al Qaeda that encouraged attacks on U.S. pipelines using weapons or hidden explosives.[54]

In 2007, the U.S. Department of Justice arrested members of a terrorist group planning to attack jet fuel pipelines and storage tanks at the John F. Kennedy International Airport.[55] In 2011, an individual planted a bomb, which did not detonate, along a natural gas pipeline in Oklahoma.[56] In

---

https://pgjonline.com/2015/05/12/cybersecurity-2015-connected-pipelines-and-proliferation-of-threats-to-infrastructure/.

49. *See* Hellmann, *supra* note 19, at 165.

50. *Id.* at 164.

51. *Id.*

52. *See* Parfomak Testimony, *supra* note 26, at 1-2.

53. *See* William Vitka, *Penn. Man Named in Alleged Terror Plot*, CBS News (Feb. 11, 2006), http://www.cbsnews.com/news/penn-man-named-in-alleged-terror-plot/.

54. *Id.*

55. Press Release, U.S. Attorney's Office, Four Individuals Charged in Plot to Bomb John F. Kennedy International Airport (June 2, 2007), https://www.justice.gov/archive/usao/nye/pr/2007/2007jun02.html.

56. Press Release, U.S. Attorney's Office, Konawa Man Sentenced for Attempting to Destroy or Damage Property Using an Explosive (Dec. 5, 2012),

2012, a man who reportedly had been corresponding with "Unabomber" Ted Kaczynski unsuccessfully attempted to bomb a natural gas pipeline in Plano, Texas.[57]

Canadian pipelines have also been targeted by physical attacks. Natural gas pipelines in British Columbia, Canada, were bombed six times between October 2008 and July 2009 by unknown perpetrators in acts classified by authorities as environmentally motivated "domestic terrorism."[58] These bombings were extremely dangerous because some of the natural gas contained deadly concentrations of hydrogen sulfide.[59]

To date, no bombings of U.S. pipelines have succeeded, but the threat of a physical attack remains credible.[60] A cyber-attack on a pipeline control system might have a similar effect as a well-placed bomb.

IV. Pipeline Integrity Issues

In addition to concerns about malicious physical damage or damage from cyber intrusions, spills due to pipeline defects, construction activity, and corrosion also present concurrent safety issues.[61] For example, the sixty-five-year-old Pegasus Pipeline recently ruptured in a subdivision of Mayflower, Arkansas, resulting in a major crude oil spill which contaminated the neighborhood and adjoining waterways.[62] The Pegasus transmission line failure was blamed on latent welding defects.[63]

---

https://archives.fbi.gov/archives/oklahomacity/press-releases/2012/konawa-man-sentenced-for-attempting-to-destroy-or-damage-property-using-an-explosive.

57. *See* Valerie Wigglesworth, *Plano Blast Suspect Corresponded with Unabomber*, Dall. Morning News (June 29, 2014), http://www.dallasnews.com/news/plano/2014/06/29/plano-blast-suspect-corresponded-with-unabomber; see also Press Release, U.S. Attorney's Office, Plano Man Guilty in Pipeline Bombing Incident (June 3, 2013), https://www.justice.gov/usao-edtx/pr/plano-man-guilty-pipeline-bombing-incident.

58. *See* Parfomak Testimony, *supra* note 26, at 2.

59. Hydrogen sulfide contaminated gas is referred to as "sour gas" in the industry. Special contingency plans must be prepared by producers in the event the deadly gas should leak from the production stream putting the public at risk.

60. *See* Parfomak Testimony, *supra* note 26, at 2.

61. *See, e.g.*, Daniel Gilbert, Big Spills from Aging Oil Pipelines, Wall St. J. (Apr. 15, 2013), https://www.wsj.com/articles/SB10001424127887323741004578418693982405224.

62. *See* Allison Sider, *Exxon Faces Fine in Spill*, Wall St. J. (Nov. 6, 2013), https://www.wsj.com/articles/SB10001424052702304448204579182331170785944 (noting 5,000 barrels of oil leaked from the May 29, 2013 rupture).

63. *See* U.S. DEP'T. OF TRANSP., PIPELINES AND HAZARDOUS MATERIALS SAFETY ADMIN., FAILURE INVESTIGATION REPORT – MOBILE PIPELINE PEGASUS RUPTURE 2 (2013), http://www.phmsa.dot.gov/staticfiles/PHMSA/DownloadableFiles/Files/FIR_redacts_marked_2016_06_16_Redacts_applied.pdf.

The Department of Transportation's ("DOT") Pipeline and Hazardous Materials Safety Administration ("PHMSA") regulates and enforces the safety standards involved in pipeline construction and operation. PHMSA accordingly documents numerous pipeline spills and leaks that occur every year due to welding failures, corrosion, excavation damage, incorrect operation, or natural events.

In a 30-month study of pipeline incidents ending in July 2012, PHMSA found 1,337 "unintentional releases" of crude oil, hazardous liquid hydrocarbons, or natural gas – more than one per day – across the nation.[64] The large number of spills and leaks adds to concerns about the integrity of the nation's pipeline system and its susceptibility to cyberattack.

A prominent release identified in the PHMSA study was the single largest onshore oil pipeline spill in U.S. history.[65] On July 25, 2010, Enbridge's 40-year-old, 30-inch pipeline ruptured near Marshall, Michigan, discharging more than 20,000 barrels of crude into suburban Talmadge Creek, ultimately fouling 40 miles of the Kalamazoo River, a tributary to Lake Michigan.[66] The cause was later identified as having occurred due to corrosion fatigue and defective welding.[67]

Analyzing pipeline failures during the period subject to the study PHMSA found that faulty materials, faulty construction, and outdated welding techniques were some of the most common causes.[68] Pipelines built in the pre-1970's era utilizing outdated technology still account for between a quarter to a third of the mileage of hazardous liquid pipelines in

64. *See* DAVID SHAW ET AL., PIPELINE AND HAZARDOUS MATERIAL SAFETY ADMINISTRATION, U.S. DEP'T OF TRANSP. FINAL REPORT NO. 12-173, LEAK DETECTION STUDY 2-5 (2012), *available at* http://www.phmsa.dot.gov/staticfiles/PHMSA/DownloadableFiles/Files/Press%20Release%20Files/Leak%20Detection%20Study.pdf (The study was conducted with pipeline engineering consultants Kiefner & Associates, Inc.).

65. *See id.* at 3-65-66; *see also* Bell, *supra* note 23, at 14.

66. *See* Bell, *supra* note 23, at 14.

67. *See id.* at 13; *see also* Tom Fowler & Daniel Gilbert, *Oil-Pipeline Cracks Evading Robotic Smart Pigs*, Wall St. J. (Aug. 16, 2013), http://www.wsj.com/articles/SB10001424127887323455104579015140328479048.

68. *See* Gilbert, *supra* note 61; *see also*); *see also* Mike Lee, *Decades of Ruptures from Defect Shows Perils of Old Pipe*, Bloomberg (Sept, 2, 2013) (noting that "faulty welds and materials accounted for 36 percent of spills and leaks on liquids pipelines between 2006 and 2010, more than any other cause, according to a Transportation Department report.").

service.[69] Replacing the low frequency electronic resistance welded pipe would cost as much as $1 million per mile, or more than $50 billion.[70]

A. Electronic Leak Detection Systems

As pipeline systems have become more automated and sophisticated, one would expect electronic leak detection systems to be very efficient at promptly identifying leaks, ruptures, spills, or abnormal operating conditions. In practice this has not been the case, as leak detection equipment tends to issue "false positives": warnings of a leak or spill when none has occurred.[71]

Studies conducted by industry regulators analyzing false alarms found that sensitivity level of monitoring equipment is typically adjusted upward to reduce the number of false signals; a lower sensitivity setting will produce more false alarms.[72] Because of this, some legitimate alarms may be discounted by the operator. In addition, the monitoring equipment may sometimes be disconnected entirely due to a high number of false alarm issuances, rendering the equipment useless in emergency leak detection.[73]

For example, in September 2016, the Colonial Pipeline, which delives product from the Gulf Coast to the Northeast United States, ruptured and spilled 8,000 barrels of gasoline.[74] The leak was inadvertently discovered by a state mine inspector days after the rupture. The automated control system gave no warnings of the potentially deadly spill.[75]

Despite the best efforts of pipeline operators and equipment manufacturers and a rapid increase in technological advancement, federal

---

69. *See* Lee, *supra* note 68.

70. *Id.* (citing an estimate by Brigham McCown, a Dallas consultant who served as Administrator of the PHMSA in 2005 and 2006.).

71. Interview with Lynn Helms, Director, North Dakota Oil & Gas Commission, in Denver Colo. (May 2016).

72. *See* PIPELINES AND HAZARDOUS MATERIAL SAFETY ADMINISTRATION, U.S DEP'T OF TRANSP., LEAK DETECTION TECHNOLOGY STUDY 8 (2007), *available at* http://www.phmsa.dot.gov/staticfiles/PHMSA/DownloadableFiles/S10-080623-002-Signed.pdf; *see also* Shaw, *supra* note 65, at 4-28.

73. Interview with Lynn Helms, *supra* note 72 (Mr. Helms indicated that the design or operation of alarm systems has been a major engineering and operational challenge for pipeline operators in the State of North Dakota as well as elsewhere, and many of the problems seen in alarm systems remain unsolved from an engineering or technology standpoint.); *see* Shaw, *supra* note 65, at 4-9.

74. Alison Sider, *Federal Regulators Investigate Colonial Pipeline Leak*, Wall St. J. (Sept. 16, 2016), https://www.wsj.com/articles/federal-regulators-investigate-colonial-pipeline-leak-1474072198?mod=pls_whats_news_us_business_f.

75. *Id.*

agency records suggest pipeline-monitoring technology designed to detect leaks is nearly as successful as a random member of the public discovering the rupture.[76] During the 20 months prior to the most recent rupture, the Colonial Pipeline had 8 pipeline spills across its 5,500-mile fuel pipeline system. According to federal data, every one of these spills went undetected by the company's primary leak-detection system.[77]

The issue of faulty leak detection systems stretches well beyond the Colonial Pipeline. According to a Reuters review of PHMSA data, since 2010, there have been at least 466 incidents in which a pipeline carrying crude oil or refined products has leaked. Of those, only 105, or 22%, were identified by an advanced detection system.[78]

A recent study of North Dakota pipelines found similar shortfalls on electronic leak detection systems.[79] The study was instigated by state regulators after a crude oil pipeline leaked for 11 days continually before being discovered by a farmer plowing his field, spilling 20,600 barrels of oil, one of the largest spills in the history of the state.[80] This incident was one of several prior leaks along the same pipeline where leak detection systems failed to give the operator notice of an operational problem.[81]

The study found that members of the public were more likely to discover a leak than an electronic warning system, leading to the conclusions that the effectiveness of leak detection technologies is marginal, except in detecting the largest of releases.[82] The report summarizes:

> Most pipeline leaks are discovered visually by people who happen to be in the area of the spill. Sensor and software

76. *See* Jarret Renshaw & Devika Krishna Kumar, *Technology designed to detect U.S. energy pipeline leaks often fails*, Reuters (Sept. 30, 2016), http://www.reuters.com/article/us-usa-pipelines-colonial-analysis-idUSKCN1200FQ.

77. *Id.*

78. *Id.*

79. *See* ENERGY & ENVTL. RESEARCH CTR., UNIV. OF N.D., LIQUIDS GATHERING PIPELINES: A COMPREHENSIVE ANALYSIS (2015).

80. Nick Smith, *Oil Leak Questions Taken up at Energy Meeting*, Bismarck Tribune (Oct. 14, 2013), http://bismarcktribune.com/bakken/oil-leak-questions-taken-up-at-energy-meeting/article_159142ee-351d-11e3-bd23-0019bb2963f4.html.

81. Interview with Lynn Helms, *supra* note 72.

82. *See* ENERGY & ENVTL. RESEARCH CTR., *supra* note 80, at xvi, 123 (finding the public discovered leaks 23% of the time during the study while electronic leak detection systems detected the leak only 17% of the time.).

> technology is evolving to meet the needs of leak detection, but they have not yet been demonstrated as reliable.[83]

Detection is critical for obvious reasons. The earlier a leak is found, the less damage caused to the environment and the operator's business. According to a Reuters review of PHMSA data, of the 361 pipeline incidents that went undetected by internal systems since 2010, a total of 141,421 barrels of petroleum products spilled, totaling $1.2 billion in property damages.[84]

The bottom line is that domestic oil and gas pipeline ruptures are not uncommon but are difficult to detect electronically or to prevent, extremely damaging to the environment, and potentially deadly. While natural corrosion or welding issues caused these aforementioned incidents, the consequences would not materially differ if a rupture was caused by cyberattacks.

B. Low Frequency Electronic Resistance Welding

In addition to the difficulties inherent in ensuring an operator is promptly notified of a pipeline spill or breach (ideally by an electronic warning system installed on the pipeline), inadequate construction standards for pipelines built before 1970 have led many of the systems on those pipelines to fail without warning.

Due to concerns regarding the large number of leaks in older pipelines, the National Institute of Standards and Technology, a technology lab run by the U.S. Commerce Department, studied the performance history of low frequency electronic resistance welded pipe commonly used by pipeline operators in construction prior to 1970.[85] The agency concluded that it was "clear that ERW pipe manufactured before about 1970 is particularly susceptible to failure." This study documented 172 welding seam failures in the pipelines carrying liquids over the previous 20 years.[86]

The research reported evidence that corrosion and metal fatigue caused by pressure changes from flowing liquids could worsen the existing pipe's weld defects.[87] The defective welds were found to be directly related to the low frequency electric resistance welding technology used during this

---

83. *Id.* at xvi.

84. *See* Renshaw, *supra* note 77.

85. *See* R.J. FIELDS ET AL., NAT'L INSTITUTE OF STANDARDS AND TECH., U.S. DEP'T OF COMM., AN ASSESSMENT OF THE PERFORMANCE AND RELIABILITY OF OLDER ERW PIPELINES 1 (1989), *available at* https://archive.org/details/assessmentofperf8941fiel.

86. *Id.* at 9-17.

87. *See Id.* at 3-4; *see also* Lee, *supra* note 68.

period.[88] Over time, the welds in low frequency electric resistance welding pipe were found to be susceptible to selective seam corrosion, hook cracks, and inadequate bonding of the seams.[89]

A manufacturing change occurred in 1970, when the low frequency welding process was superseded by high frequency electric resistance welding in pipeline construction. High frequency welds are higher quality, which is statistically less likely to fail during normal operating conditions.[90]

Damage from ruptured crude oil transmission lines are more visible to the public eye, but natural gas leaks can also cause serious safety issues and property damage. In the past two decades, the government has recorded "more than 2,000 accidents on natural gas transmission lines across the U.S., resulting in 46 deaths, 181 injuries and $1.8 billion in property damage."[91]

The previously mentioned explosion of a 54-year-old Pacific Gas & Electric natural gas distribution pipeline in the densely populated San Francisco suburb of San Bruno illustrates such danger. The explosion left behind massive destruction, leaving a crater, igniting fierce fires, destroying 38 homes, killing 8 individuals, and injuring many more.[92] During the investigation, federal investigators reported that they found numerous defective welds in the pipeline.[93]

Many of these serious pipeline incidents have several elements in common: old systems, welding methods no longer accepted as safe or allowed in new pipeline construction, defective materials, and in many cases signs of corrosion due to the age of the system.[94] To put the issue into perspective, more than half of the nation's pipelines are at least 40 years old.[95] These systems were constructed before current regulatory standards, technologically advanced corrosion protection systems and x-ray testing

88. *Id.* at 3-5.

89. *Id.* at 3.

90. *See id.* at 4-5; *see also* Dallas Morning News, "*Welding Flaw Raises Pipeline Risk*" (September 15, 2013) page 2A.

91. *See Explosive history prompts pipeline safety proposal to address gaps in oversight*, Associated Press (March 17, 2016), http://www.pennlive.com/nation-world/2016/03/gas_pipeline_safety_proposal.html.

92. *See* Bell, *supra* note 23, at 14 (The explosion and fire was so intense local television coverage thought an airplane had crashed into the subdivision.).

93. *See* Jason Dearen, *Report on Calif Pipeline Blast Finds Weld Defects*, Associated Press (Jan. 21, 2011), http://archive.boston.com/business/articles/2011/01/21/report_on_calif_pipeline_blast_finds_weld_defects/.

94. *See* Lee, *supra* note 68.

95. *Id.*

were established.[96] Compared to modernly constructed pipelines, pipelines constructed under these past unsound regulatory conditions are particularly vulnerable to cyberattacks.

C. Preventative Testing For Leaks and Defects

Due to the number of pipeline incidents, and the aging pipeline infrastructure, both industry and regulators have explored preventative methods to identify and test for pipeline integrity and defects. The Battelle Memorial Institute conducted a study of existing pipeline systems for PHMSA, analyzing 280 cases in which electric-welded pipes failed between 1950 and 2005.[97] The research group concluded that the most efficient way to identify a weld defect was to remove the crude oil, gasoline, or natural gas and pump water into the pipeline in a process called "hydrostatic testing."[98]

This testing process raises the internal pipeline pressure above the operating norm to check for leaks that may be apparent when additional stresses are added to the system.[99] Such tests are costly and require a company to shut down and drain the line of its contents. The Battelle study found that such testing can actually weaken the electric welded seams due to expansion and contraction, increasing the chance of failure when the pipeline is placed back in service.[100]

In addition to hydrostatic testing, many pipelines are inspected using a "smart pig" device. This device is inserted into a pipeline and transmits or records data as it is pushed through the pipeline.[101] Studies indicate these devices have a reliability of around 90% in identifying potential problems. Unfortunately, smart pigs tend to miss corrosion or tiny cracks that occur in a pipe's longitudinal welded seam, which is a common occurrence in older low frequency welded pipe.[102]

---

96. *Id.*

97. *See* BATTELLE MEM'L INST., FINAL SUMMARY REPORT AND RECOMMENDATIONS FOR THE COMPREHENSIVE STUDY TO UNDERSTAND LONGITUDINAL ERW SEAM FAILURES (2013), *available at* https://primis.phmsa.dot.gov/matrix/FilGet.rdm?fil=8501&s=564166D08D9B4BDC945E61DE0EF85D94&c=1.

98. *Id.* at A-12.

99. *See Fact Sheet: Hydrostatic Pressure Testing*, Pipeline & Hazardous Materials Safety Admin., https://primis.phmsa.dot.gov/comm/FactSheets/FSHydrostaticTesting.htm.

100. *See* BATTELLE MEM'L INST., *supra* note 97, at 17-18.

101. *See Fact Sheet: In-Line Inspections (Smart Pig)*, Pipeline & Hazardous Materials Safety Admin., https://primis.phmsa.dot.gov/comm/FactSheets/FSSmartPig.htm.

102. *See* Lee, *supra* note 68; *see also* BATTELLE MEM'L INST., *supra* note 97, at 16.

The unsteady state of the physical pipeline infrastructure in the U.S. makes facilities extremely vulnerable to damage in the event of a cyberattack. Simply altering operating pressures, flow direction, or flow rates have led to pipeline spills and ruptures in older legacy pipelines, resulting in massive spills.[103] If a cyberattack manages to alter the operating parameters in a way that exceeds pipeline design limitations, high probability exists that substantial damage will occur.

V. Federal Regulatory Structure

The federal regulatory structure currently in place addressing pipeline cybersecurity issues is one of recent origin given the relatively recent nature of the threat. The origin of federal programs addressing oil and gas pipeline cybersecurity issues stems primarily from federal legislation promulgated to address pipeline safety issues.[104]

Under the statutes, the DOT was given primary authority to regulate key aspects of interstate pipeline safety including design, construction, operations, maintenance, and spill response. Pipeline regulation is overseen by the DOT's PHMSA.[105]

Furthermore, as the U.S. economy modernized, in 1998, the Clinton administration issued a presidential directive addressing the growing concerns over the vulnerability of the nation's infrastructure with regards to both physical and cyberattacks.[106] Pursuant to the directive, the DOT holds responsibility for pipeline *security* in addition to its safety responsibilities.[107] Under this authority, working with the Department of Energy, industry groups, and state pipeline safety organizations, the DOT "promoted the development of consensus standards for security measures."[108]

---

103. *See* Gilbert, *supra* note 61.

104. The Natural Gas Pipeline Safety Act of 1968, Pub. L. No. 90-481, 82. Stat. 720 (codified as amended as 49 U.S.C. § 60101 et seq. (2016)) and the Hazardous Liquid Pipeline Act of 1979, Pub. L. No. 96-129 (codified as amended as 49 U.S.C. § 60101 et seq. (2016)) are two of the principal early acts establishing the federal role in pipeline safety.

105. The DOT's website contains information with regard to the various sectors they regulate, including the PHMSA (available at https://www.transportation.gov/home).

106. *See* WHITE HOUSE, PRESIDENTIAL DECISION DIRECTIVE-63: CRITICAL INFRASTRUCTURE PROTECTION (1998), *available at* https://clinton.presidentiallibraries.us/items/show/12762.

107. *Id.* at 10.

108. *See* Parfomak Testimony, *supra* note 26, at 4; *see e.g.*, American Petroleum Inst., Nat'l Petrochemical & Refiners Ass'n., *Security Vulnerability Assessment Methodology for*

After the events of September 11, 2001, the Transportation Security Administration ("TSA") was established with the passage of the Aviation and Transportation Security Act. .[109] The act vested in the TSA responsibility for security in "all modes of transportation," including "security responsibilities over . . . modes of transportation that are exercised by the Department of Transportation."[110] Thus, the TSA interpreted the act as granting the DOT's pipeline security authority under the Clinton presidential directive within the TSA.[111] However, with the TSA focusing primarily on aviation regulation early on, the DOT maintained a prominent regulatory role through circulating formal guidance developed in cooperation with the pipeline industry associations, defining the DOT's recommendations and implementation expectations .[112]

On November 25, 2002, President Bush signed the Homeland Security Act of 2002.[113] This Act created the Department of Homeland Security and transferred the TSA and its pipeline security regulation authority from the DOT to the Department of Homeland Security, where it remains today.[114] The existing regulatory structure will continue to evolve as cybersecurity threats become a larger issue to both the economy and the public.

A. TSA Pipeline Regulation

Under the current statutory and regulatory system, the TSA is vested with the authority to issue pipeline security and cybersecurity regulations.[115] But the TSA has not issued specific regulations or cybersecurity mandates out of a concern that mandatory standards may encourage pipeline operators to adopt a lower standard of protection than many industry participants have already voluntarily adopted.[116]

---

the Petroleum and Petrochemical Industries (2003), https://www.nrc.gov/docs/ML0502/ML050260624.pdf.

109. President Bush signed the Aviation and Transportation Security Act, 49 U.S.C. § 40101, in November 2001.

110. 49 U.S.C. § 114(d)(2) (2001).

111. PAUL W. PARFOMAK, CONG. RESEARCH SERV., RL31990, PIPELINE SECURITY: AN OVERVIEW OF FEDERAL ACTIVITIES AND CURRENT POLICY ISSUES 14 (2004), https://fas.org/sgp/crs/RL31990.pdf

112. *See* Parfomak Testimony, *supra* note 26, at 4; *see also* TRANSP. SEC. ADMIN., PIPELINE SECURITY GUIDELINES 1 (2011), https://www.tsa.gov/sites/default/files/tsapipelinesecurityguidelines-2011.pdf.

113. 6 U.S.C. §§ 101-1533 (2002).

114. *Id.* at § 203 (The DOT retained pipeline safety and inspection responsibilities).

115. *See* PARFOMAK, *supra* note 21, at 1.

116. *Id.* at 7-8.

Instead of issuing bright line regulations, the TSA has addressed cybersecurity regulatory concerns through issuance of voluntary "best practice" recommendations and guidance.[117] Voluntary, as opposed to mandatory, regulations have been controversial since most energy sector regulatory requirements have historically been mandatory in nature. In addition, some have questioned the limited amount of TSA resources dedicated to the pipeline cybersecurity effort in light of the extent and ubiquitous nature of the nation's pipeline system.[118] For example, the TSA's pipeline security division as of 2012 only staffed 13 full-time employees[119] and as of 2016 the pipeline security division staff would "account for less than 2% of the agency's surface transportation security staff under the proposed FY2017 budget."[120] Additional responsibilities such as formal rulemaking and enforcement would not be possible at current staffing and budgetary levels.[121]

Because the TSA has chosen to rely on voluntary guidance to regulate the industry, the industry is essentially self-regulated. For example, the Interstate Natural Gas Association of America maintains its own extensive cybersecurity guidelines for natural gas pipeline control systems. Similarly the American Petroleum Institute ("API") maintains an industry standard for oil pipeline control system security.[122]

Essentially, the voluntary standards promulgated by industry insiders are just as authoritative as those set forth by the TSA. As an example, to defend systems against cyberattacks the API recommends that pipeline operators follow "API standard 1164."[123] This standard requires operators to keep systems for pipeline operations separate from business systems.[124] API Standard 1164 also requires pipeline operators to follow precautionary

117. *Id.* at 6.

118. *See* Parfomak Testimony, *supra* note 26, at 12-13.

119. *See* PARFOMAK, *supra* note 21, at 8.

120. *See* Parfomak Testimony, *supra* note 26, at 13.

121. PARFOMAK, *supra* note 21, at 9-10.

122. *See* American Petroleum Inst., *supra* note 108.

123. *See Pipelines: Securing the Veins of the American Economy*: *Hearing Before the H. Subcomm. on Transp. Sec.*, 114th Cong. 2 (2016) (statement of Andrew Black, President and CEO, Ass'n of Oil Pipelines), http://docs.house.gov/meetings/HM/HM07/20160419/104773/HHRG-114-HM07-Wstate-BlackA-20160419.pdf.

124. *Id.*

measures and implement preventative practices to ensure sound security practices are in place.[125]

The pipeline industry generally supports voluntary standards and recommendations. Many firms in the sector are concerned that regulators will adopt mandatory standards. These mandatory standards could establish a standard of care against which alleged negligence could be measured. Industry associations have also been concerned that specific voluntary or mandatory standards could expose the pipeline operator to liability in the event of a cybersecurity breach.[126]

B. 2014 Cybersecurity Framework

Recognizing the cybersecurity threat to all sectors of the domestic economy, President Obama issued an executive order addressing this issue in February 2013.[127] The order expanded public-private information sharing and required the Commerce Department's National Institute for Standards and Technology (NIST) to prepare a voluntary "Cybersecurity Framework".[128]

The Framework provides a voluntary procedure to identify cybersecurity best practices utilized by industry, determine the overall state of an organization's cyber risk management practices, and structure management recommendations for organizations to mitigate those risks.[129]

The Cybersecurity Framework attempts to set out consensus standards to provide a flexible and cost-effective approach for companies to enhance

---

125. For a draft version of API Standard 1164 see *Pipeline SCADA Security*, American Petroleum Inst., http://ballots.api.org/pipeline/ballots/docs/Std1164_SCADASecurity_ballotdraft_3Ed_20161028.pdf.

126. *See Cyber Threats and Security Solutions: Hearing Before the H. Subcomm. on Energy and Commerce*, 113th Cong. 10 (2013) [hereinafter McCurdy Testimony] (statement of Dave McCurdy, President and CEO, American Gas Association), http://docs.house.gov/meetings/IF/IF00/20130521/100883/HHRG-113-IF00-Wstate-McCurdyD-20130521.pdf.

127. Improving Critical Infrastructure Cybersecurity, 3 C.F.R. § 13636 (2013), *available at* https://www.gpo.gov/fdsys/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf.

128. *Id.* at 217-219; *see generally Why you should adopt the NIST Cybersecurity Framework*, PwC (May 2014), http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf.

129. *See* 3 C.F.R. § 13636.7; *see generally* Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?:Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 Tex. Int'l L.J. 303 (2015), *available at* http://www.tilj.org/content/journal/50/14%20SHACKELFORD%20PUB%20PROOF.pdf.

cybersecurity. Owners and operators of critical infrastructure could in theory use this program to assesses and manage cyber risk.[130]

It is important to note that the Cybersecurity Framework is not specifically focused on the energy sector or pipeline industry. As such, its recommendations are more broadly applicable to sectors of the economy that may not face the dangers inherent in transporting flammable, and many times explosive, materials over long distances.[131] Compliance with the Framework recommendations remains voluntary.

VI. Tort Liability

In a case involving damages from a pipeline incident caused by a cybersecurity breach, the plaintiff will have the burden of proving liability as well as the obligation to quantify any damages incurred.[132] Due to the complexity of the pipeline system, construction methods, operations, data control systems, and cybersecurity, most cases will require expert testimony.[133]

The energy sector is heavily regulated at both the federal and state level with numerous standards, orders, and enforcement actions. These regulations have been used in many cases to establish a standard of conduct expected of industry participants. [OBJ][OBJ][134] Violation of these regulations or statutes can be pursued by both agencies as well as by private litigants requesting damages, and it is not unusual for the courts to adopt the regulation as a standard of care.[135]

Cybersecurity threats are evolving in nature and severity, and there is a lack of mandated standards and regulations applicable to industry participants. As a result, the liability of a pipeline operator for a breach of security may not be as straightforward as the liability consideration when a

130. *See Why you should adopt the NIST Cybersecurity Framework*, *supra* note 128.

131. *See* Weiss v. Thomas & Thomas De. Co., 680 N.E.2d 1239, 1242 (Ohio 1997) (setting a higher standard of care because natural gas is a "dangerous commodity" with "dire consequences" when the flammable and explosive gas escapes containment) (quoting Suiter v. Ohio Valley Co., 225 N.E.2d 792, 792 (Ohio 1967)).

132. See Corbello v. Iowa Prod., 850 So. 2d 686 (La. 2003) (finding the plaintiff had established environmental liability and had quantified damages by a preponderance of the evidence).

133. *See infra* note 259.

134. 16 Tex. Admin. Code, § 3.9 (2014) (regulating the disposal of produced water from oil and gas wells and the permitting requirements for underground injection control wells).

135. Generally regulatory agencies can impose a fine for violations. Damages to injured parties are awarded to claimants in state or federal court.

pipeline ruptures due to corrosion or a construction defect. We expect that some of the basic legal principles addressed in historical pipeline cases might be extended to cases that deal with cybersecurity incidents.

For example, cases generally have held that natural gas utilities or pipelines have been held to a higher standard of care than normal due to the danger they present to the public.[136] Though damages from a pipeline breach are generally linked to foreseeable harms, the issue is a question of fact and damages are sometimes held unrecoverable, especially when "extraordinary use" of the surface leads to injury.[137] Should a pipeline be at risk of a rupture, the operator likely will have a duty to warn the public of the danger. Voluntary industry standards can in some cases be utilized to evaluate whether a pipeline has met its duty of care to the public. We will analyze these issues in detail below.

A. Pipeline Operator's Duty of Reasonable Care

The standard of care generally required of defendants in tort actions is that of a "reasonably prudent" person.[138] The inquiry defines "what a reasonable person would have done under similar circumstances," which will "necessarily depend on the particular facts of each case."[139] A particular industry custom or practice is probative of what conduct would be considered reasonable under the circumstances.

Courts examining the issue of a pipeline operator's duty of care have held that an entity which transports or distributes natural gas is under a duty to exercise a "higher degree" of care than normal due to the dangers inherent in handling flammable, explosive, and toxic substance.[140]

The duty of reasonable care has been defined as requiring a company distributing natural gas for domestic use to deliver such gas at a safe, uniform pressure, to institute and maintain an efficient system of oversight

136. *See Weiss*, 680 N.E.2d at 1242 ("It is a matter of common knowledge that although gas is a highly useful commodity it is also a dangerous commodity with a marked tendency to escape from its proper confines."); *see also* Nw. Ohio Natural Gas Co., v. First Cong. Church of Toledo, 184 N.E. 512, 513 (Ohio 1933) ("By reason of the highly dangerous character of gas and its tendency to escape, a gas company must use a degree of care, to prevent the escape of gas from its pipes, commensurate with the danger.").

137. *See* Phillips Pipeline Co. v . Razo, 420 S.W.2d 691, 693-695 (Tex. 1967).

138. *See* Sears, Roebuck & Co. v. Midcap, 893 A.2d. 542, 554 (Del. 2004); *see also* Robelen Piano Co. v. DiFonzo, 169 A.2d 240, 244, (Del. 1961).

139. *Sears, Roebuck & Co.*, 893 A.2d at 554.

140. Margay Oil Corp. v. Jamison, 59 P.2d 790, 792 (Okla. 1936); *Weiss*, 680 N.E.2d at 1242; Schell v. OXY USA Inc., 822 F. Supp. 2d 1125, 1136 (D. Kan. 2011).

to ensure that the pressure continues to remain safe and uniform, and to provide a "prompt remedy for accidents."[141] Other cases have held that the duty to produce and distribute gas in a reasonably safe and prudent manner did require the distributors to warn consumers of dangerous leaks by odorizing the gas they supply.[142]

Because of the precarious character of crude oil and natural gas and the multitude of dangers involved in distributing the fuel, most courts have refrained from explicitly stating the specific degree of care required.[143] The policy has been that those handling flammable and explosive substances should be required to exercise such a "degree of care" and caution as is "commensurate" with the known danger.[144] Whether or not defendant exercised such care is an issue of fact, which should be submitted to a jury.[145]

Plaintiffs in such cases have argued that in addition to common law rules, applicable regulations may establish a standard of care or benchmark for the pipeline operator.[146] This is especially true for natural gas distribution systems where the pressure, odorization, quality, and a host of other factors are strictly regulated. "Reasonable care" in the distribution of

---

141. *See* Indiana Natural & Illuminating Gas Co. v. Long, 59 N.E. 410 (Ind. Ct. App. 1901) (holding a municipal water utility liable for tortious injury to private rights where the utility failed to supply water to a greenhouse at the agreed upon pressure for a number of days); *see also* City of Huntingburg v. Morgen 162 N.E. 255 (Ind. Ct. App. 1928) (en banc).

142. *See* Roberts v. Ind. Gas & Water Co., 218 N.E.2d 556 (Ind. Ct. App. 1966) (en banc), on rehearing, 221 N.E.2d 693 (Ind. Ct. App. 1966) (en banc); Richmond Gas Co. v. Baker, 45 N.E. 1049, 1050 (Ind. 1897) (holding a gas utility owed duty to all persons who might be injured to use ordinary and adequate care in delivering substance to residence); City of Indianapolis v. Walker, 168 N.E.2d 228 (Ind. Ct. App. 1961) (requiring a gas utility to exercise ordinary care in maintenance of line); *see also* S. Ind. Gas Co. v. Tyner, 97 N.E. 580, 585 (Ind. Ct. App. 1911) (finding a gas company owed duty to customers, patrons, and occupants of buildings where it supplied agency to use care commensurate with danger to which it exposed persons or property.

143. S. Tex. Nat. Gas Gathering Co. v. Guerra, 469 S.W.2d 899, 909 (Tex. App. 1971) ("In the absence of a standard of care established by statute or regulation, the courts have said that a pipeline owner or operator is under a duty to exercise that degree of care which a prudent man would exercise under all the circumstances, or care which is commensurate with the dangerous character of the pipeline and necessary to protect the public from foreseeable injury therefrom. An analysis of the cases shows that the duty and standard of care that a pipeline operator owes to a person on the surface of a pipeline right of way varies according to the status of the parties and the use of the property.").

144. Oklahoma Gas & Elec. Co. v. Oklahoma R.R. Co., 188 P. 331, 332 (Okla. 1920).

145. Goodwin v. Enserch Corp., 949 F.2d 1098, 1107 (10th Cir. 1991).

146. Brozak v. Broad, No. 12 CVC-05-6865, 2013 Ohio Misc. LEXIS 10294, at * (Ohio Ct. Of Common Pleas 2013).

natural gas can be established by examining the applicable regulations since the utility is transporting and delivering a dangerous instrumentality.[147]

For example, in *South Eastern Indiana Natural Gas Co. v. Ingram*, the plaintiffs allege that a utility that "supplied gas to them experienced a partial interruption of service to its customers in the form of a reduction in line pressure."[148] While the utility's employees responded to phone calls in the early hours of the interruption, at no time did they attempt to notify the plaintiff that she should switch to an emergency source of heat.[149]

Hours later, when the greenhouse temperature was zero degrees and the contents of it were a total loss, the loss of heat caused by the reduction in line pressure was discovered.[150] The plaintiff alleged that the utility's "negligence in not warning them to switch to an emergency source of heat was the proximate cause of their damages, which included a loss of inventory, profits, customers, labor, interest on borrowed money, and additional damages."[151]

The court in *South Eastern Indiana Natural Gas* noted that the duty owed—the obligation to conform to a certain standard of care—was a question of law for the court.[152] It determined that the gas supplier had a duty to its customers.[153] The question of whether the natural gas utility met that duty of reasonable care in proving natural gas services to customers was a question of fact.[154]

B. Duty and Foreseeability

The question of whether a duty arises to third parties also turns on the question of whether the damage from a pipeline cyberattack is foreseeable.[155] In Texas, the courts set out the general rule that "a party should not be held responsible for the consequences of an act which ought

147. S. Ind. Gas Co. v. Tyner, 97 N.E. 580, 580 (Ind. Ct. App. 1911).

148. 617 N.E.2d. 943, 946 (Ind. Ct. App. 1993).

149. *Id.* at 946.

150. *Id.*

151. *Id.*

152. *Id.* at 951.

153. *Id.* ("[T]he duty of a utility to use reasonable care in the distribution of gas is imposed by law for a second reason: the utility conveys a dangerous instrumentality.").

154. Id. at 950.

155. *See* Isaacs v. Huntington Mem'l Hosp., 695 P.2d 653, 664 (Ca. 1985) ("It is well settled that an owner of land has a duty 'to take affirmative action to control the wrongful acts of third persons which threaten invitees where the [owner] has reasonable cause to anticipate such acts and the probability of injury resulting therefrom.'" (citation omitted)).

not reasonably to have been foreseen."[156] A party will not be negligent whether it does or fails to do an act when the possible resulting injury is not anticipated.[157] Neither a legal nor a moral obligation exists to guard against that which cannot be foreseen.[158]

In *Wohlford v. American Gas Production Co.*, a landowner sued an oil and gas producer for damages to his land, grass, and cattle that resulted from the "blowing" of a gas well.[159] As the court explained, gas wells must be occasionally cleaned.[160] Here, the company operating the well was attempting to remove accumulations of dirt, liquids, sand, rocks, water, and shale in the wellbore, which had caused a serious decrease in the flow of gas.[161] By venting the natural gas well into the atmosphere twice a year, the operator removed these obstacles to production.[162]

This method of venting into the atmosphere was the "most efficient way to clean gas wells" and was customarily used in the industry unless "salt water, oil, or perhaps some other objectionable or poisonous substance" was present.[163] The "more pressure and velocity," the "more rubbish blown out of the well" according to the court.[164]

Though the operator had used this method of cleaning the well for years with no apparent damage to the surface or animals, in this case, arsenic was within the mix of substances blown from the well; the discharge poisoned the landowner's cattle.[165] As this was the "first known case of arsenic damage from a gas well," the operator had no knowledge of the arsenic, had never encountered this problem in prior operations on the property, and nearby wells had not experienced such an issue.[166]

Applying Texas law, the court found the arsenic and the resulting cattle deaths were not foreseeable, therefore a negligence claim was not

156. Texas & Pac. R.R. Co. v. Bigham, 38 S.W. 162, 163 (Tex. 1896).
157. *Id.* at 163.
158. *Id.*
159. 218 F.2d 213, 214 (5th Cir. 1955).
160. *Id.* at 216.
161. *Id.* ("The gas passing through the earth's formations carries with it dirt, liquids, shale, rocks, oil and water which settle around the wells and materially reduce the flow of gas. The general practice is to open the top of the pipe and 'let her blow'. More pressure and velocity are thereby obtained and more rubbish blown out of the well.").
162. *Id.*
163. *Id.*
164. *Id.*
165. *Id.*
166. *Id.*

actionable.[167] In the court's holding, it found that when the presence of arsenic in the well admittedly could not have been foreseen, no duty rested on the appellee to protect the appellant from the unknown and unheard of hazard of arsenic in the well.[168]

No duty arises when "unusual, improbable, extraordinary and freakish" events result in an accident according to the courts, but the question of foreseeability is determined on a case-by-case factual basis.[169]

In *Phillips Pipe Line Co. v. Razo,* the court held that the use of heavy equipment on a small, rarely used, private road or trail in muddy terrain was an extraordinary use of the surface.[170] Here, when a bulldozer struck a buried pipeline that exploded and subsequently caught fire, the court held that such extraordinary use and injury was not foreseeable.[171] Similar to the *Wohlford* case, the *Phillips* court held the defendant was not liable for damages since the pipeline operator's duty of ordinary care did not extend to "hold the pipeline operator liable for every conceivable contact with the pipeline."[172]

In examining the issue of foreseeability courts have noted that "it is necessary to review the 'totality of the circumstances' including the nature, condition and location of the defendant's premises."[173] Foreseeability involves the jury examining the "general character of the event or harm . . . not its precise nature or manner of occurrence."[174]

In *South Texas Natural Gas Gathering Co. v. Guerra,* an employee of a cattle company was injured when a bulldozer operator struck a natural gas pipeline while constructing agricultural ponds on a ranch.[175] Applying Texas law, the court noted

---

167. *Id.* at 217.

168. *Id.* (citing Carey v. Pure Distributing Corp., 124 S.W.2d 847, 849 (holding it is required "the injury be of such a general character as might reasonably have been anticipated.")); *see also* San Antonio & A.P. R.R. Co. v. Behne, 231 S.W. 354, 356 (Tex. Comm'n App. 1921, judgm't adopted).

169. Larco Drilling & Exploration Corp. v. Brown, 267 So. 2d 308, 310 (Miss. 1972); Ann M. v. Pac, Plaza Shopping Center, 863 P.2d 207 (Ca. 1993) (where the court noted that a duty "will be imposed only where conduct can be reasonable anticipated").

170. 420 S.W.2d 691 (Tex. 1967).

171. *Id.*

172. *Id.* at 695.

173. 420 S.W.2d 691.

174. Isaacs v. Huntington Mem'l Hosp., 695 P.2d 653, 661 (Ca. 1985) (quoting Bigbee v. Pac. Tel. & Tel. Co., 665 P.2d 947 (Ca. 1983)).

175. 469 S.W.2d 899 (Tex. App. 1971).

> In the absence of a standard of care established by statute or regulation, the courts have said that a pipeline owner or operator is under a duty to exercise that degree of care which a prudent man would exercise under all the circumstances, or care which is commensurate with the dangerous character of the pipeline and necessary to protect the public from foreseeable injury therefrom. An analysis of the cases shows that the duty and standard of care that a pipeline operator owes to a person on the surface of a pipeline right of way varies according to the status of the parties and the use of the property.[176]

The *South Texas* court concluded that at the time of the accident, the question of whether the use of the surface was "extraordinary" was an issue for the jury to decide.[177] If the surface use was determined to be extraordinary the pipeline operator might not anticipate such use, and the duty to mark the route of the pipeline might not exist.[178]

In *Prudential Fire Insurance Co. v. United Gas Corp.*, the defendant gas company installed a meter to a gas line on the plaintiff's property. The facts were disputed as to whether the defendant installed the meter with defects or whether the plaintiff damaged the meter causing a gas leak which subsequently caused an explosion destroying the plaintiff's property.[179]

The plaintiff alleged that even if they had damaged the meter, the gas company did not ensure there was a safeguard in place for the plaintiff's line to protect it from the actions of third parties.[180] The plaintiff argued that the gas company knew or should have known in placing the meter where it was on the line it would be exposed to the public activity.[181]

The court held that, even in light of the facts most favorable to the gas company, the cause was reasonably foreseeable on the basis that the gas company failed to provide adequate safeguards, considering the volatility of the commodity that they were providing and given that they had actual knowledge that the meter was unprotected and exposed to third party damage.[182]

---

176. *Id.* at 909 (citing the annotation at 30 ALR 3rd 670).
177. *Id.* at 910.
178. *Id.*; *See also* Phillips Pipe Line Co. v. Razo, 420 S.W.2d 691 (Tex. 1967).
179. 199 S.W. 2d 767, 768 (Tex. 1946).
180. *Id.* at 769.
181. *Id.*
182. *Id.* at 773.

Where damages might be extensive, or where a dangerous situation could result in substantial loss to the public, the courts have further considered policy considerations when examining the question of foreseeability.[183]

In *Lammle v. Gappa Oil Co.*, after an uncapped propane line caused an explosion that leveled the plaintiff's home and caused the plaintiff to sustain severe injuries, she filed suit against numerous parties involved in the renovation project including the furnace manufacturer and the wholesale suppliers of propane gas.[184]

The court in *Lammle* held that "while propane gas is a dangerous product and explosions are conceivable, public policy does not support imposing a duty on wholesale suppliers with respect to every conceivable explosion that could occur at any point in the supply chain."[185] Continuing, the court noted, "the fact that a certain event, such as a propane gas explosion, is conceivable does not mean it is foreseeable in the legal sense."[186]

A number of cases have determined that foreseeability does not require that similar events had occurred in the past.[187] Even with an absence of prior similar events occurring an event could be foreseeable, and hence a duty to protect would be created.[188] The concept of foreseeability is "elastic" according to some courts.[189] Where the extent of harm is elevated the courts note they will be more likely to determine the damage was foreseeable.[190]

---

183. *See* Foss v. Kincade, 746 N.W.2d 912, 915-16 (Minn. App. 2008) where the court held "a duty will not lie when the connection between the damage-causing event and the alleged negligent act is 'too remote to impose liability as a matter of public policy,'" (quoting Germann v. F.L. Smithe Mach. Co., 395 N.W.2d 922, 924 (Minn. 1986)).

184. Lammle v. Gappa Oil Co., A08-0582, 2009 Min. App. LEXIS 42, at *2 (Min. Ct. App. Jan. 13, 2009).

185. *Id.* at *11.

186. *Id.* at *10 (quoting *Foss*).

187. *See* Isaacs .v Huntington Mem'l Hosp., 695 P.2d 653, 659 (Cal. 1985) which noted "the fortuitous absence of prior injury does not justify relieving defendant from responsibility for the foreseeable consequences of its acts," (quoting Weirum v. RKO Gen., Inc., 539 P.2d 36 (Ca. 1975)).

188. *See Isaacs*, 695 P.2d at 659; *Ann M.*, 863 P.2d at 214.

189. Lopez v. McDonald's Corp., No. D004619, 1987 Cal. App. LEXIS 1913, at *510 (4th Dist. July 9, 1987).

190. *Isaacs*, 695 P.2d at 659.

C. Foreseeabiility and Cyberintrusion

Industry surveys indicate that many energy sector executives believe the chance of a cybersecurity breach of U.S. infrastructure is a relatively likely occurrence over the next several years, with the potential for loss of life.[191] But, to date, no domestic pipelines have been subject to a cyberattack causing a leak or damages.[192]

Where an event causing damage is 'extraordinary', 'improbable' or 'freakish' in nature the courts have been reluctant to find they were foreseeable, and therefore have held that there was not a duty to protect.[193] The courts have noted that foreseeability is a question of fact, which depends on the specific circumstances.[194]

With the lack of mandatory cybersecurity standards issued by the TSA,[195] many pipeline operators who comply with voluntary industry standards, TSA recommendations, and guidelines could attempt to argue they did not expect—in the normal course of business—to encounter a cybersecurity breach. According to this industry argument, the occurrence of a damage-causing cyber intrusion would be highly unusual and unexpected. It would follow that since the event was not foreseeable, no duty would exist on the part of the pipeline operator to protect the public or third parties.[196]

Offsetting this argument is the fact that many jurisdictions addressing the foreseeability question have adopted the view that a prior event similar to the incident causing harm is not required to establish foreseeability.[197] Under this line of reasoning, the fact no cybersecurity intrusions have occurred on pipeline systems to date would not be a strong argument that the event would not be foreseeable. Further, because the courts have indicated that the concept of foreseeability is somewhat flexible, when the potential harm to the public is elevated (as it would be in situations where pipelines containing flammable and explosive substances are compromised) the event is more likely to be determined to be foreseeable.[198]

---

191. Krancer et al., *supra* note 2.

192. *See* Parfomak Testimony, *supra* note 26, at 3.

193. *Larco*, 267 So. 2d 308, 310 (Miss. 1972); *Ann M.*, 863 P.2d at 207.

194. *Isaacs*, 695 P.2d at 659.

195. *See* Parfomak Testimony, *supra* note 26, at 10.

196. *See Isaacs*, 695 P.2d at 659; *see also* Lopez v. McDonald's Corp., No. D004619, 1987 Cal. App. LEXIS 1913, at *512 (4th Dist. July 9, 1987).

197. *Isaacs*, 695 P.2d at 659.

198. *Id.*

It is important to keep in mind that, in addition to the numerous pipeline cybersecurity incidents that have already occurred in other areas of the world, the number and sophistication of cyberattacks in general have been increasing domestically, furthering the notion that such an act would be considered foreseeable.[199]

Regarding foreseeability, it is likely that—in most factual scenarios—a court could determine a pipeline cyber intrusion would be expected to occur based on the trends discussed previously. In light of such a finding, the pipeline would have a foreseeable duty to protect third parties and the public from damage.

D. Duty to Warn of Danger

If a pipeline system has been compromised by a cyberattack, does the operator have a duty to warn customers or the public about the potential harm that might be caused by such an intrusion?

In *American Cyanamid Co. v. Sparto*,[200] a Texas court addressed the question of whether a petroleum refinery located just north of Fort Worth had a duty to warn downstream parties that the plant had dumped high volumes of salts into the Trinity River as part of the refining process.[201]

The use of the high saline downstream water for irrigation was deleterious to the landowner's crops, stunted crop growth, and created a permanent salt crust on the soil.[202] The court held that since the refinery created the environmental hazard at issue it had a duty to warn the downstream farmers about the danger of utilizing the polluted waters.[203]

In the case of *Ford Motor Co. v. Dallas Power & Light Co.*, the court addressed the issue of whether a party who controlled the floodgates to a dam or cooling pond for an electrical generation station had a duty to warn those downstream about an impending flood after a major storm.[204] The court noted, "Texas law does recognize a duty to warn on the part of the

199. *See* Parfomak Testimony, *supra* note 26, at 2-3.

200. 267 F.2d 425 (5th Cir. 1959).

201. *Id.*

202. *Id.* at 427 (noting that the polluted process water contained several chemical compounds that were primarily ammonium and sodium sulphate).

203. *Id.* at 429. ("[T]he appellant's right was not an unlimited one, it follows that if the exercising of that right created a risk of injury to the appellees which might have been averted by a warning, there was a duty to warn and the failure so to do would constitute actionable negligence.").

204. 499 F.2d 400 (5th Cir. 1974).

person who creates a dangerous situation, although without negligence on his part."[205]

In *Buchanan v. Rose*, the court stated, "We think it may also be said that if one by his own acts, although without negligence on his part, creates a dangerous situation . . . the one creating the same must give warning of the danger or be responsible for the consequences."[206]

Because the defendant in *Buchanan* did not create the dangerous situation and was "merely aware of the danger" when he failed to warn fellow drivers, the Supreme Court of Texas did not find him liable.[207] Mere knowledge of a "dangerous situation or helpless condition of another person" creates only a moral—not legal—duty to warn or render aid.[208]

The *Buchanan* court lists as an example that one who, "without negligence, strikes a trolley pole with his automobile and causes it to fall across the road is liable for failure to protect others from injury thereby."[209] Clarifying, the court noted that "the defendant by his own act created the dangerous situation[]" and therefore had a duty to warn.[210]

In the case where a third party cyber intrusion occurs, even without pipeline operator negligence, a strong argument could be made that, since the pipeline system in the hands of a cyberattacker presents a danger to the public, a warning must be issued by the pipeline system operator. Failure to issue such a warning could be considered negligence.

E. Negligence Per Se

A number of theories can be asserted by a party damaged by a cybersecurity breach, although an allegation of negligence will likely be the most common. A plaintiff who seeks to utilize a negligence cause of action must prove (a) the existence of a legal duty, (b) violation of that duty, (c) damages, (d) and proximate causation which results in the injury.[211]

Generally, the cases dealing with pipelines have held that ruptures or breaches tend to be foreseeable, and since the pipeline is transporting a

---

205. *Id.* at 412.

206. 159 S.W. 2d 109, 110 (Tex. 1942).

207. *Id.*

208. *Ford*, 499 F.2d at 412; Boyer v. Gulf, Colorado & Santa Fe R.R., 306 S.W.2d 215, 222 (Tex. App. 1957).

209. *Buchanan*, 159 S.W. 2d at 110.

210. *Id.*

211. USAA Cas. Ins. Co. v. PM Terminals, Inc., No. 3:12cv868, 2013 U.S. Dist. LEXIS 139942, at *8 (E.D. Va. Aug. 6, 2013) (quoting Kellermann v. McDonough, 684 S.E.2d 786, 790 (Va. 2009)).

hazardous, flammable, and in many cases explosive material, such cases have held the pipeline operator to a higher standard of care.[212]

To establish a breach of this duty, the plaintiff can use a violation of a rule, ordinance, or statute under a theory of negligence per se. The tort concept of negligence per se is expressed in the Restatement (Second) of Torts as "the unexcused violation of a legislative enactment or an administrative regulation which is adopted by the court as defining the standard of conduct of a reasonable man, is negligence in itself."[213]

The theory of negligence per se is subject to some limitations, but can make a plaintiff's case easier to prove assuming the court adopts the regulations or statutes as an appropriate method to establish a reasonable standard of conduct.

In *Rodriguez v. American Cyanamid Co.*, the court noted that a "statutory violation is negligence per se if the court allows the statute to stand in for the reasonable standard of conduct. The infraction then constitutes a deviation from the standard of care, and the plaintiff need not prove the existence of a duty and a breach."[214]

Numerous early energy cases applying the negligence per se theory were brought in Oklahoma after the enactment of a statute that addressed the standard of care required for "produced water," the largest waste product generated from most oil and gas wells.[215] The statute—enacted in 1910, shortly after Oklahoma become a state—provided that wastes should be transported from the well premises and "in no case" should the waste or saltwater be allowed to "flow over the land."[216]

In their review of this statute and the duty of care it imposed on an oil and gas operators, Oklahoma Courts have noted that "[t]he statute is a penal statute….[a] violation of the statute constitutes negligence and a violation

212. Weiss v. Thomas & Thomas De. Co., 680 N.E.2d 1239, 1239 (Ohio 1997).

213. RESTATEMENT (SECOND) OF TORTS § 288B (1965).

214. 858 F.Supp. 127, 129 (D. Ariz 1994) (citing the Restatement (Second) of Torts § 286 (1965) that a "court may adopt as the standard of conduct of a reasonable man the requirements of a legislative enactment or an administrative regulation whose purpose is found to be exclusively or in part: (a) to protect the particular class of persons which includes the one whose interest is invaded, (b) to protect the particular interest which is invaded, and (c) to protect that interest against the kind of harm which has resulted, and (d) to protect that interest against the particular hazard from which the harm results.").

215. Regulatory Determination for Oil and Gas and Geothermal Exploration, Development and Production Wastes, 53 Fed. Reg. 25447 (July 6, 1988).

216. 52 Okla. Stat. §296 (2016).

resulting in an injury to another constitutes actionable negligence".[217] Subsequent cases have found that oil and gas well operators that allow salt water wastes from oil or gas wells to run over the surface of the land are liable to surface owners if they suffer injury.[218]

Some courts have further noted that if statutes or regulations are used to establish a duty of care, those statutes and regulations will be strictly construed.[219] For example, the Oklahoma statute above applies to waste from a producing oil or gas wells, and when a plaintiff attempted to use it to establish a standard of care for pollution from a refinery or a pipeline, the court held that the statute was inapplicable.[220] In addition to their strict construction, statutes and regulations have been held as prospective in nature and cannot be utilized retroactively to establish a duty of care.[221]

In *Sinclair Prairie Oil Co. v. Stell*, a man drove his truck off a bridge and drowned in a pool of salt water, which had been deposited in violation of the oil and gas waste pollution statute.[222] In the subsequent lawsuit for wrongful death, the court noted that the applicable statute was strictly construed, with the intent of the statute to address environmental issues from oil and gas wells, and so dismissed the claim of negligence per se.[223]

The negligence per se doctrine is also limited by other exceptions. For example, in the Texas case, *Murfee v. Phillips Petroleum Co.*, the court noted that the applicable Texas Railroad Commission regulation stated "pollution was prohibited" was too general in nature to establish a standard of conduct the violation would create negligence per se.[224]

The *Murfee* case also noted that, in this instance, a thick limestone barrier, which impeded the intrusion of polluted fluids, effectively protected the area where groundwater allegedly was polluted by oil and gas

---

217. Wilcox Oil Co. v. Walters, 284 P.2d 726, 729 (Okla. 1955) (citing Tex. Co. v. Belvin, 251 P.2d 804 (Okla. 1952)).

218. Sun Oil Co. v. Hoke, 169 P.2d 753 (Okla. 1946); Wilcox Oil Co. v. Walters, 284 P.2d 726 (Okla. 1955); Cleary Petroleum, Inc. v. Copenhaver, 476 P.2d 327 (Okla. 1970).

219. *Wilcox Oil Co.*, 284 P.2d at 729.

220. *See* Johnson Oil & Refining Co. v. Carnes, 51 P.2d 811, 812 (Okla. 1935); *see also* Gulf Pipe Line Co. v. Alred, 77 P.2d 1155 (Okla. 1938) (applying the rule from *Johnson*).

221. Hicks v. Humble Oil and Refining Co., 970 S.W.2d 90, 94 (Tex. App. 1998).

222. 124 P.2d 255, 257-58 (Okla. 1942).

223. *Id.* at 258.

224. 492 S.W.2d 667 (Tex. App. 1973). Strictly construed, this regulation would also effectively create strict liability in Texas for pollution or spills, something the Texas Supreme Court expressly rejected in Turner v. Big Lake Oil Company, 96 S.W.2d 221 (Tex. 1936).

activity.[225] Because of this observation, the *Murfee* case can be said to further stand for the fact that—even if a statute or regulation applies—the court may grant an exception to liability on the negligence per se theory when the facts support such a cite.[226]

In *Schwartzman, Inc. v. Atchison, Topeka & Santa Fe Railway Co*., the plaintiff filed suit under a number of environmental statutes asking for monetary damages.[227] The court noted in that case the "[a]ssertion of a negligence cause of action predicated on an alleged violation of a statute is little more than an attempt to assert a private cause of action for damages by privately enforcing the statute in question," holding that the intent of the legislation was to protect the public from environmental harm and not to provide a private cause of action for damages.[228]

Since cybersecurity regulations generally are voluntary in nature,[229] it follows that there is not a set of specific mandates available for a court to examine and adopt as a reasonable standard of care. Due to the voluntary scope of the cybersecurity regulations, and the lack of specific statutory or regulatory mandates, the question arises if voluntary standards can serve to establish a standard of care the violation of which would constitute negligence per se.

F. Voluntary Versus Mandatory Standards

One of the key aspects of the pipeline cybersecurity regulations, is that they are deemed voluntary by nature, and have therefore allowed flexibility in decision making. Many of the industry players and associations, as well as regulators, prefer this voluntary environment because it allows them to be flexible in meeting their duty to the public, their employees, and shareholders.[230]

Regulators, for the most part also prefer voluntary standards since they claim it allows them to adjust to rapidly changing cyber and technological threats and developments.[231] The evolving nature of cyberattacks creates an

225. *Murfee*, 494 S.W.2d at 673-74.

226. *Id.*

227. 857 F. Supp. 838 (D.N.M. 1994).

228. *Id.* at 848 (noting the overriding criterion is legislative intent). *But see* Hicks v. Humble Oil and Refining Co., 970 S.W.2d 90 (Tex. App. 1998) (noting the court need to analyze the intent of the regulators in adopting certain oil and gas rules to determine if the plaintiff could use those regulations to establish a duty of care).

229. *See* Parfomak Testimony, *supra* note 26, at 9.

230. *See* McCurdy Testimony, *supra* note 126, at 5-7.

231. *Id.* at 6. (McCurdy's testimony also explains that the TSA Pipeline Security Division has not issued mandatory cybersecurity regulations for the pipeline industry due in

environment which makes it difficult to timely propose firm rules and standards, much less adopt such rules after the delays inherent in the rule making notice, comment, and hearing process.

Due to the relatively new nature of the cybersecurity threat there are few cases specifically addressing the use of voluntary cybersecurity standards as establishing a standard of care, but courts have reviewed voluntary standards or industry customs in other cases. These decisions have generally concluded that the voluntary standards do not automatically establish a specific standard of care in a negligence case.[232] Rather, the breach of a voluntary standard constitutes "one more piece of evidence upon which the jury could decide whether the defendant acted as a reasonably prudent person in the circumstances of the case."[233]

A defendant would be "free to argue that the [voluntary] standard is unduly demanding, either in general or in the particular instance, and that the standard does not reflect actual industry practice, [ ] that the standards are not of a type that a reasonably prudent person would employ,"[234] or that a violation of that standard is excused by the factual circumstance of the particular case.[235]

In addition, it has been recognized that industry organizations or regulators who possess differing degrees of expertise—especially in technology-driven areas like cyber security—are the parties who develop the voluntary standards. In some cases, industry participants have conflicting interests; hence the voluntary rules may not reflect a consensus viewpoint as to what should be considered reasonable or effective.

Voluntary standards may be considered "simply recommendations written by experts" who may not themselves be available for cross-examination," according to one court.[236] The merits of the voluntary standards are "for the jury's consideration like any other evidence in the case."[237]

---

part to the effective partnership they have with industry and the fact the voluntary program appears to be effective in addressing current threats.).

232. Getty Petroleum Mktg., Inc. v. Capital Terminal Co., 391 F.3d 312, 326 (1st Cir. 2004) (Lipez, J., concurring).

233. *Id.* at 326 (quoting Boston & Me. R.R. v. Talbert, 360 F.2d 286, 290 (1st Cir. 1966)).

234. *Id.*

235. *Id.*

236. *Id.* (citing Boston & Me. R.R. v. Talbert, 360 F.2d 286, 290 (1st Cir. 1966)).

237. *Id.* at 326-27.

Plaintiffs have also utilized specific company policies, as they have utilized voluntary industry or regulator standards, in an attempt to establish an applicable standard of care.[238] Courts have noted that company policies "represent some evidence of a reasonably prudent standard of care"[239] but have also recognized that "voluntary written policies and procedures do not themselves establish a *per se* standard of due care."[240] Similarly, violations of safety policy or codes are evidence of negligence, but do not conclusively establish negligence nor do they establish a negligence per se standard of conduct.[241]

Many cases follow the reasoning in *Sears, Roebuck & Co. v. Midcap,* in which a propane kitchen range exploded destroying a home and killed one of the occupants.[242] The plaintiff requested to enter into evidence an industry wide safety program, which outlined the installation and maintenance of propane equipment, the violation of which they claimed would establish negligence.[243] The plaintiffs argued the program established a reasonable standard of conduct for parties involved in servicing this industry.[244]

The voluntary program in *Sears, Roebuck & Co.* involved the limited inspection of residential gas systems and the connected appliances.[245] At the time of the trial, no state or federal agency had made the standards mandatory and the standards did not specifically recommend specific details under what conditions the inspection should be completed.[246] The question of if additional periodic inspections should be conducted was not addressed.[247] Additionally, the court noted that different industry

238. Brown v. Cedar Rapids & Iowa City R.R. Co., 650 F.2d 159 at 163 (8th Cir. 1980) ("The trend also favors admission of industry or voluntary association codes and *of private codes adopted by an employer*." (emphasis added)).

239. Hall v. Toreros, II, Inc., 626 S.E. 2d 861, 866 (N.C. App. 2006) (quoting Klassette v. Mecklenburg County Area Mental Health, 364 S.E.2d 179, 183 (NC Court of Appeals 1988))

240. *Id.* at 183.

241. *See* Norris v. Zambito, 520 S.E.2d 113, 118 (N.C. App. 1999) ("A violation of voluntarily adopted safety policies is merely some evidence of negligence and does not conclusively establish negligence."); *see also* Wilson v. Lowe's Asheboro Hardware, Inc., 131 S.E.2d 501, 505 (1963) (voluntary adoption of safety code "some evidence that a reasonably prudent person would adhere to the requirements of the code.").

242. 893 A.2d 542, 545 (Del. 2004).

243. *Id.*

244. *Id.* at 554.

245. *Id.* at 555.

246. *Id.*

247. *Id.*

participants had implemented the standard in differing ways.[248] For these reasons the court did not adopt the voluntary standard as establishing a standard of care since there was no evidence that the program had been adopted as a standard by the gas supply industry.[249]

In *Linden v. CNH America,*, the question arose as to whether the violation of an industry adopted safety code established negligence.[250] The court held that the jury could take the non-conformance with code into consideration in the deliberations, but the non-conformance was not in itself an indication the defendant had violated a standard of care.[251] Generally, courts have treated safety standards as "factual evidence that the court may admit or exclude based on ordinary evidentiary principles."[252]

In *Brown v. Cedar Rapids & Iowa City Railway Co.*, a railroad employee acting as a lookout, was injured when he was struck by a switching stand that was constructed too close to the tracks.[253] At trial the jury considered a proposed regulation, which was not in effect at the time of the accident, as evidence of negligence.[254] On review the court noted recent trends in standards:

> The trend in federal as well as state court is to allow admission of advisory safety codes promulgated by governmental authority as showing an acceptable standard of care….The trend also favors admission of industry or voluntary association codes and of private codes adopted by an employer . . . . Such codes do not have the force of law and do not establish negligence per se.[255]

In *Michaels v. Mr. Heater, Inc.*, a question arose with regard to expert testimony alleging that the defendant's failure to comply with a voluntary

248. *Id.*
249. *Id.*
250. 673 F.3d 829 (8th Cir. 2012).
251. *Id.* at 838.
252. *See* Getty Petroleum Mktg., Inc. v. Capital Terminal Co., 391 F.3d 312 (1st Cir. 2004) (citing Miller v. Yazoo Mfg. Co., 26 F.3d 81, 83-84 (8th Cir.1994) (where voluntary standard was properly admitted)); *See also* Matthews v. Ashland Chem., Inc., 770 F.2d 1303, 1310–11 (5th Cir.1985) (where voluntary standards were properly excluded); Boston & Me. R.R. v. Talbert, 360 F.2d 286, 290 (1st Cir.1966) (where voluntary standards were properly admitted); Dickie v. Shockman, No. A3–98–137, 2000 WL 33339623, *3 (D.N.D. July 17, 2000) (admitting expert testimony regarding voluntary standards)).
253. 650 F.2d 159, 163 (8th Cir. 1981).
254. *Id.*
255. *Brown*, 650 F.2d at 163 (citations omitted).

industry standard was negligence.[256] In that case, a propane heater exploded in a vehicle, resulting in critical injury to the driver.[257] The plaintiffs alleged that the product was defectively designed.[258] With regard to the expert testimony the court referred to and relied upon the Federal Rules of Evidence to determine if the expert testimony would assist the trier of fact in making a decision.[259]

The *Michaels* court determined that the expert testimony was admissible since it assisted the court in understanding the alleged defect in the propane fueled heating equipment.[260] The court further noted the voluntary industry standards were admissible and could be considered in light of the specific facts, although they were not conclusive evidence of negligence.[261]

VII. Conclusion

The pipeline infrastructure in the United States is dated and vulnerable to malicious cyberattacks. As illustrated by cyberattacks on pipelines outside of the United States, these incidents could cause substantial damage and, according to experts, the frequency with which our domestic pipeline systems have been targeted for cyberattacks is only increasing. Many predict it is only a matter of time until a major cyber event involving our energy infrastructure occurs in the U.S.

It is difficult to establish a regulatory framework to insure that the energy infrastructure is protected from cyberattacks due to the developing and evolving nature of the threat. If specific mandates were adopted by the regulatory agencies, such regulations likely would be too inflexible to property address the cyber threat, and such mandates might even hinder an operator's response or leave them exposed to malicious activity.

---

256. 411 F. Supp 2d 992 (W.D. Wis. 2006).

257. *Id.* at 995.

258. *Id.*

259. FED. R. EVID. 702 states "If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case."

260. *Michaels*, 411 F. Supp 2d at 996-97.

261. *Id.* (citing Getty Petroleum Marketing, Inc. v. Capital Terminal Co., 391 F.3d 312, 326 (1st Cir. 2004) (Although "voluntary standards do not irrefutably establish the standard of care in a negligence case . . . they constitute one more piece of evidence upon which the jury could decide whether the defendant acted as a reasonably prudent person in the circumstances of the case.")).

Voluntary cybersecurity standards similar to those currently in place are probably best suited to the environment, especially where these standards are adopted with joint industry and regulator participation while being reviewed and regularly updated.

Ultimately, should a cyberattack occur and a pipeline system is breached causing third party damage, general principles adopted by the courts in historical tort cases involving pipelines will most likely apply. For instance, the operator of a hydrocarbon pipeline most likely will be held to a higher standard of care with regard to the cybersecurity issues due to its duty to protect the public and environment from the explosive, toxic, and flammable nature of the substances being transported.

Even if the attack is deemed terrorism, damage caused from a cybersecurity attack involving a pipeline or SCADA system will most likely be deemed foreseeable due to the number of global incidents that have occurred over the last decade. Existing case law indicates that the pipeline operator will have a duty to warn the public of the dangers presented should a cyberattack occur. Therefore, voluntary standards most likely will be admitted by the courts to allow an expert witness to establish a negligence cause of action, though the court may not necessarily adopt these voluntary standards to define a standard of care for the operator in a negligence per se claim.