# PIPELINES: SECURING THE VEINS OF THE AMERICAN ECONOMY

# HEARING

BEFORE THE

## SUBCOMMITTEE ON TRANSPORTATION SECURITY

OF THE

## COMMITTEE ON HOMELAND SECURITY
## HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

APRIL 19, 2016

**Serial No. 114–64**

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PUBLISHING OFFICE
22–757 PDF WASHINGTON : 2016

## COMMITTEE ON HOMELAND SECURITY

Michael T. McCaul, Texas, *Chairman*

Lamar Smith, Texas
Peter T. King, New York
Mike Rogers, Alabama
Candice S. Miller, Michigan, *Vice Chair*
Jeff Duncan, South Carolina
Tom Marino, Pennsylvania
Lou Barletta, Pennsylvania
Scott Perry, Pennsylvania
Curt Clawson, Florida
John Katko, New York
Will Hurd, Texas
Earl L. "Buddy" Carter, Georgia
Mark Walker, North Carolina
Barry Loudermilk, Georgia
Martha McSally, Arizona
John Ratcliffe, Texas
Daniel M. Donovan, Jr., New York

Bennie G. Thompson, Mississippi
Loretta Sanchez, California
Sheila Jackson Lee, Texas
James R. Langevin, Rhode Island
Brian Higgins, New York
Cedric L. Richmond, Louisiana
William R. Keating, Massachusetts
Donald M. Payne, Jr., New Jersey
Filemon Vela, Texas
Bonnie Watson Coleman, New Jersey
Kathleen M. Rice, New York
Norma J. Torres, California

Brendan P. Shields, *Staff Director*
Joan V. O'Hara, *General Counsel*
Michael S. Twinchek, *Chief Clerk*
I. Lanier Avant, *Minority Staff Director*

---

## SUBCOMMITTEE ON TRANSPORTATION SECURITY

John Katko, New York, *Chairman*

Mike Rogers, Alabama
Earl L. "Buddy" Carter, Georgia
Mark Walker, North Carolina
John Ratcliffe, Texas
Michael T. McCaul, Texas *(ex officio)*

Kathleen M. Rice, New York
William R. Keating, Massachusetts
Donald M. Payne, Jr., New Jersey
Bennie G. Thompson, Mississippi *(ex officio)*

Krista P. Harvey, *Subcommittee Staff Director*
John Dickhaus, *Subcommittee Clerk*
Cedric C. Haynes, *Minority Subcommittee Staff Director*

# CONTENTS

Page

## STATEMENTS

## WITNESSES

## APPENDIX

# PIPELINES: SECURING THE VEINS OF THE AMERICAN ECONOMY

---

**Tuesday, April 19, 2016**

U.S. House of Representatives,
Committee on Homeland Security,
Subcommittee on Transportation Security,
*Washington, DC.*

The subcommittee met, pursuant to call, at 2:24 p.m., in Room 311, Cannon House Office Building, Hon. John Katko [Chairman of the subcommittee] presiding.

Present: Representatives Katko, Rogers, Carter, Ratcliffe, and Rice.

Mr. Katko. The Committee on Homeland Security, Subcommittee on Transportation Security will come to order. The subcommittee is meeting today to examine how the Transportation Security Administration works with pipeline stakeholders to secure this critical infrastructure.

I now recognize myself for an opening statement. Over 2.6 million miles of pipeline run through the United States carrying oil and natural gas operated by approximately 3,000 companies. The integrity of this complex network of pipelines is critical not only to our economy, but in keeping our cars running and our stoves burning. Following the creation of the Department of Homeland Security, responsibility for pipeline security shifted to the TSA, while the Department of Transportation retained responsibility for pipeline safety. Although the terms safety and security are often used interchangeably, the root causes for concern behind each of these concepts are fundamentally different and warrant differing approaches.

While safety focuses on preventing and responding to accidents, security aims to thwart malicious actors with ill intentions from damaging or disrupting pipeline operations. The threat to pipeline security has been deemed relatively low by the intelligence community. This is largely due to security measures put in place by operators and the extent to which a vast majority of the U.S. pipeline network is buried underground. However, we must remain diligent. Just because terrorists have not yet targeted pipelines for an attack does not mean they will not in the future. In addition to physical attacks, we must also guard against cyber attacks.

Our adversaries, including North Korea, China, Russia, and Iran have shown a proclivity for launching sophisticated cyber attacks against U.S. companies, banks, and critical infrastructure. In March the Justice Department indicted members of Iran's Revolutionary Guard for hacking the operational control system of a small dam in my home State of New York.

While there is no evidence that hackers had been able to penetrate the industrial systems of pipelines, there have been several high-profile incidents where the systems of global energy companies have been compromised and sensitive information fell into the wrong hands. As hackers become more sophisticated, we cannot discount the possibility that they may one day seek to intrude on the industrial control systems, disrupting the flow of oil and natural gas. Although TSA has the authority to regulate pipeline security, they have chosen instead to pursue a more collaborative approach with the industry. That could serve as a model for other parts of the Government. However, I am concerned that TSA has not issued any updates to the pipeline security guidelines since 2011.

I look forward to learning more about how TSA and industry stakeholders work together to ensure the security of our Nation's pipelines. Although I must say I am preliminarily encouraged that all sides seem to be happy with the current arrangement.

I would like to thank everyone for being here today, and I look forward to hearing the testimony from our distinguished panel of witnesses.

With that I now recognize my Ranking Member of the subcommittee, the gentlewoman from New York, Miss Rice, for any statements she may have.

[The statement of Chairman Katko follows:]

## STATEMENT OF CHAIRMAN JOHN KATKO

APRIL 19, 2016

Over 2.6 million miles of pipeline run through the United States carrying oil and natural gas operated by approximately 3,000 companies. The integrity of this complex network of pipelines is critical not only to our economy, but in keeping our cars running and our stoves burning.

Following the creation of the Department of Homeland Security, responsibility for pipeline security shifted to the Transportation Security Administration while the Department of Transportation retained responsibility for pipeline safety. Although, the terms "safety" and "security" are often used interchangeably, the root causes for concern behind each of these concepts are fundamentally different and warrant differing approaches. While safety focuses on preventing and responding to accidents, security aims to thwart malicious actors with ill intentions from damaging or disrupting pipeline operations.

The threat to pipeline security has been deemed relatively low by the intelligence community. This is largely due to security measures put in place by operators and the extent to which a vast majority of the U.S. pipeline network is buried underground. However, we must remain diligent. Just because terrorists have not yet targeted pipelines for an attack does not mean they will not in the future.

In addition to physical attacks, we must also guard against cyber attacks. Our adversaries, including North Korea, China, Russia, and Iran, have shown a proclivity for launching sophisticated cyber attacks against U.S. companies, banks, and critical infrastructure.

In March, the Justice Department indicted members of Iran's Revolutionary Guard Corps for hacking the operational control system of a small dam in my home State of New York. While there is no evidence that hackers have been able to penetrate the industrial control systems of pipelines, there have been several high-profile incidents where the systems of global energy companies have been compromised and sensitive information fell into the wrong hands. As hackers become more sophisticated, we cannot discount the possibility that they may one day seek to intrude on the industrial control systems, disrupting the flow of oil and natural gas.

Although TSA has the authority to regulate pipeline security, they have chosen instead to pursue a more collaborative approach with the industry, that could serve as a model for other parts of the Government.

However, I am concerned that TSA has not issued an update to the Pipeline Security Guidelines since 2011. I look forward to learning more about how TSA and industry stakeholders work together to ensure the security of our Nation's pipelines.

I would like to thank everyone for being here today. I look forward to hearing the testimony from our distinguished panel of witnesses.

Mr. KATKO. With that I now recognize my Ranking Member of the subcommittee, the gentlewoman from New York, Miss Rice, for any statements she may have.

Miss RICE. Thank you, Mr. Chairman. Thank you for convening this hearing. I would also like to thank the witnesses for coming to talk with us about the current state of pipeline security, as well as the major threats facing the industry, and the biggest vulnerabilities that need to be addressed. I understand that it has been several years since this committee last held a hearing on our Nations pipelines. So I think it is important that we are here today to examine how TSA implements and enforces policies regarding pipeline security, as well as the steps the industry takes on their own initiative.

Last week we held a roundtable briefing with stakeholders in the oil and natural gas pipeline industry. I was impressed by the confidence they have in their relationship with TSA. They appreciate that TSA understands there is no one-size-fits-all approach to pipeline security. I was pleased to hear that TSA and the pipeline industry have that kind of constructive partnership with open and honest communication. Because there is no question that pipelines are a potential target.

With more than 2.5 million miles of pipelines carrying gas, oil, and other hazard materials across the country, an attack against a pipeline could cause major commercial and environmental damage. So it is important that the policies and procedures we put in place, to secure pipelines, reflect the magnitude of that threat. I understand that rather than issuing regulations, TSA has implemented several initiatives like the Corporate Security Review, during which TSA visits the largest pipeline operators to examine their facilities and their security plans. I am interested to learn more about that process, how often TSA conducts theses reviews, and what resources they use to inspect pipeline operators.

I would also like to know whether or not TSA receives input from DHS's National Protection and Programs Directorate when dealing with pipeline security, both physical and cyber. During our roundtable discussion last week, it was clear that when it comes to eliminating vulnerabilities, stakeholders are focused primarily on cybersecurity. Pipeline operators use supervisory control and data acquisition systems to remotely control and observe pipelines.

Cybersecurity is a top priority right now for many industries and Government agencies. So I hope to hear more from our witnesses about what pipeline operators are doing to better protect their cyber infrastructure, and how TSA is supporting those efforts, and helping to raise awareness about cyber vulnerabilities. I know that TSA holds regular conference calls with stakeholders so they can share information and keep open lines of communication.

I would like to hear from our witnesses about how that process works, and whether TSA is providing the actionable information they need to be prepared to identify and address vulnerabilities.

Thankfully there have not been any successful attacks against our Nation's pipeline systems. But there have been attempts, like in 2007 when 3 men were arrested for plotting to blow up fuel tanks and pipelines at JFK Airport in New York, which is just outside my district. We must remain cognizant of the fact that terrorists are always looking to exploit vulnerabilities, and our pipelines are a major target. So we have to always stay 2 steps ahead.

Again, I want to thank all of our witnesses for being here to assist us in that effort. I thank Chairman Katko for convening this hearing. I look forward to a productive discussion today. I yield back the balance of my time.

[The prepared statement of Ranking Member Rice follows:]

### STATEMENT OF RANKING MEMBER KATHLEEN M. RICE

APRIL 19, 2016

I understand that it's been several years since this committee last held a hearing on our Nation's pipelines, so I think it's important that we're here today to examine how TSA implements and enforces policies regarding pipeline security, as well as the steps the industry takes on their own initiative.

Last week, we held a roundtable briefing with stakeholders in the oil and natural gas pipeline industry, and I was impressed by the confidence they have in their relationship with TSA. They appreciate that TSA understands there's no one-size-fits-all approach to pipeline security.

I was pleased to hear that TSA and the pipeline industry have that kind of constructive partnership with open and honest communication—because there's no question that pipelines are a potential target. With more than 2.5 million miles of pipelines carrying gas, oil, and other hazardous materials across the country, an attack against a pipeline could cause major commercial and environmental damage. So it's important that the policies and procedures we put in place to secure pipelines reflect the magnitude of that threat.

I understand that rather than issuing regulations, TSA has implemented several initiatives like the Corporate Security Review—during which, TSA visits the largest pipeline operators to examine their facilities and security plans. I'm interested to learn more about that process—how often TSA conducts these reviews, and what resources they use to inspect pipeline operators.

I'd also like to know whether or not TSA receives input from DHS's National Protection and Programs Directorate when dealing with pipeline security—both physical and cyber. During our roundtable discussion last week, it was clear that when it comes to eliminating vulnerabilities, stakeholders are focused primarily on cybersecurity. Pipeline operators use supervisory control and data acquisition systems to remotely control and observe pipelines.

Cybersecurity is a top priority right now for many industries and Government agencies—so I hope to hear more from our witnesses about what pipeline operators are doing to better protect their cyber infrastructure, and how TSA is supporting those efforts and helping to raise awareness about cybervulnerabilities.

I know that TSA holds regular conference calls with stakeholders so they can share information and keep open lines of communication. I'd like to hear from our witnesses about how that process works, and whether TSA is providing the actionable information they need to be prepared to identify and address vulnerabilities.

Thankfully, there have not been any successful attacks against our Nation's pipeline systems, but there have been attempts—like in 2007, when 3 men were arrested for plotting to blow up fuel tanks and pipelines at JFK Airport in New York just outside my district. We must remain cognizant of the fact that terrorists are always looking to exploit vulnerabilities, and our pipelines are a major target—so we have to always stay 2 steps ahead.

Mr. KATKO. Thank you, Miss Rice. Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

### STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

APRIL 19, 2016

The Transportation Security Administration is well-known for its role in commercial aviation security. However, TSA's responsibility includes oversight of various modes of transportation, including transportation of natural gasses, hazardous liquids, and toxic inhalation hazard pipelines across the United States.

This hearing today is long overdue. The subcommittee has not had a public hearing on pipeline security since 2010. In the past, this committee has stated its intention to explore pipeline security under our oversight functions, but time and again, the committee pivoted to other matters.

Although there have been no successful attacks on U.S. pipelines, it is important that the United States remain vigilant. Pipelines are subject to both physical and cyber attacks.

With nearly 3 million miles of pipelines traversing the Nation, it is important that the committee learns what the both the public and private sectors are doing to ensure that bad actors who want to cause devastation to our Nation's economy and critical infrastructure are not able to do so.

I would like to thank the witnesses for appearing before us today and providing testimony on this subject. Ms. Proctor, I look forward to learning more about how TSA works with the private sector to address pipeline security vulnerabilities.

Mr. Black, I look forward to understanding the perspective of the owners and operators of pipelines, and particularly hearing about your concerns with your response plan submissions and the potential impact of those who wish to do us harm gaining access to the sensitive information contained within these plans.

Ms. Judge, I was pleased to read in your testimony that you believe TSA's role in facilitating the public-private partnership to address pipeline security offers a healthy level of collaboration, support, and achievement. I look forward to your testimony.

Finally, Mr. Parfomak, your expertise regarding the landscape of pipeline security and the historical context and possible implications is greatly appreciated, and we thank you for participating in the discussion today.

Mr. KATKO. We are pleased to have a distinguished panel of witnesses before us today on this important topic.

The first witness, Ms. Sonya Proctor, currently serves as a surface division director in the Office of Security Policy and Industry Engagement at TSA. That must take a very big business card to fit that title on there. The Chair now recognizes Ms. Proctor to testify.

## STATEMENT OF SONYA PROCTOR, SURFACE DIVISION DIRECTOR, OFFICE OF SECURITY POLICY AND INDUSTRY ENGAGEMENT, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. PROCTOR. Thank you. Chairman Katko, Ranking Member Rice, and Members of the subcommittee thank you for the opportunity to appear before you today to discuss the TSA's role in securing our Nation's pipelines. The pipeline network is critical to the U.S. economy. More than 2.5 million miles of pipelines transport natural gas, refined petroleum products, and other commercial products throughout the country. As evidenced by recent attacks in Brussels and elsewhere, the terrorist threat is increasingly complex and diffuse, with the potential for actors to become radicalized and carry out an attack with little warning.

An attack against a pipeline system could result in loss of life and significant economic effects. To ensure we remain vigilant, TSA works closely with the pipeline industry which consists of approximately 3,000 private companies who own and operate the Nation's pipelines. Pipeline system owners and operators maintain direct responsibility for securing pipeline systems.

TSA's role is to support owners and operators by identifying threats, developing security programs to address those threats, and encouraging and assisting the implementation of those security programs. Along with the Department of Transportation, TSA co-chairs the Pipeline Government Coordinating Council to facilitate information sharing and coordinate on security assessments, training, and exercises. TSA and DOT's Pipeline and Hazardous Materials Safety Administration, or PHMSA, work together to integrate pipeline safety and security priorities, as measures installed by pipeline owners and operators often benefit both safety and security.

TSA engages pipeline industry stakeholders through the Pipeline Sector Coordinating Council, which provides a primary point of entry for industry representatives to discuss a range of pipeline issues with Government. To assist pipeline owners and operators in securing their systems, TSA has developed and distributed security training for industry employees and partners. Additionally, with the assistance of industry and Government partners, TSA developed the TSA Pipeline Security Guidelines to provide a structure for industry to voluntarily use in developing security plans and programs.

Assessment results show that implementation of this guidance has enhanced critical infrastructure security throughout the country. TSA works with industry partners to assess and mitigate vulnerabilities through exercises, assessments, and inspections. TSA facilitates intermodal security training and exercise program, or I–STEP, exercises to help pipeline operators test their security plans, prevention and preparedness capabilities, threat response, and cooperation with first responders. To identify shortfalls in pipeline security and enhance industry practices, TSA conducts corporate and physical security reviews with pipeline operators.

Pipeline owners and operators welcome these voluntary reviews, as they appreciate the value of secure systems. TSA has conducted over 140 corporate security reviews of operators' security policies, plans, and programs since 2002, and over 400 physical security reviews of critical facilities since 2008.

TSA supports Department of Homeland Security cybersecurity efforts in support of the National Institute of Standards and Technology cybersecurity framework, and is coordinating a voluntary cyber assessment program, with the Federal Energy Regulatory Commission, to examine pipeline operators' cybersecurity programs. TSA works closely with the pipeline industry to identify and reduce cybersecurity vulnerabilities, including facilitating Classified briefings to increase industry's awareness of cyber threats.

In conclusion, TSA works closely with industry and Government stakeholders to secure the Nation's pipeline systems from terrorist attacks through the development and implementation of intelligence-driven, risk-based policies, and programs.

Thank you for the subcommittee's support of TSA's goals. I look forward to your questions.

[The prepared statement of Ms. Proctor follows:]

## PREPARED STATEMENT OF SONYA PROCTOR

APRIL 19, 2016

Good afternoon Chairman Katko, Ranking Member Rice, and distinguished Members of the subcommittee. I appreciate the opportunity to appear before you today to discuss the Transportation Security Administration's (TSA) role in securing our Nation's pipeline systems.

The pipeline network is critical to the economy and security of the United States. More than 2.5 million miles of pipelines transport natural gas, refined petroleum products, and other commercial products throughout the country. In addition to the pipelines themselves, the system includes critical facilities such as compressor and pumping stations, metering and regulator stations, breakout tanks, and the automated systems used to monitor and control them. As evidenced by recent attacks in Brussels, Paris, and elsewhere, the terrorist threat has grown increasingly complex and diffuse, with the potential for terrorist actors to become radicalized and carry out an attack with little warning. An attack against a pipeline system could result in loss of life and have significant economic effects.

To ensure we remain vigilant, TSA works closely with the pipeline industry, which consists of approximately 3,000 private companies who own and operate the Nation's pipelines. Because they are usually unstaffed, securing pipeline facilities requires a collaborative approach across Government and industry. TSA has established effective working relationships to ensure strong communication and sharing of intelligence, training resources, best practices, and security guidelines. Pipeline system owners and operators maintain direct responsibility for securing pipeline systems. TSA's role is to support owners and operators by identifying threats, developing security programs to address those threats, and encouraging and assisting the implementation of those security programs.

### STAKEHOLDER ENGAGEMENT

TSA has established a productive public-private partnership with Government partners and the pipeline industry to secure the transport of natural gas and hazardous liquids. On behalf of the Department of Homeland Security (DHS), TSA serves as a co-Sector-Specific Agency alongside the Department of Transportation (DOT) and the United States Coast Guard (USCG) for the transportation sector. As part of the DHS-led Critical Infrastructure Partnership Advisory Council framework, TSA and DOT co-chair the Pipeline Government Coordinating Council to facilitate information sharing and coordinate on activities including security assessments, training, and exercises. TSA and DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA) work together to integrate pipeline safety and security priorities, as measures installed by pipeline owners and operators often benefit both safety and security.

TSA engages pipeline industry stakeholders through the Pipeline Sector Coordinating Council (SCC), which provides a primary point of entry for industry representatives to discuss a range of pipeline security strategies, policies, activities, and issues with Government. To eliminate the need for multiple meetings with the same security partners, TSA worked closely with the Department of Energy to ensure the Pipeline SCC also functions as the Pipeline Working Group within the Energy Oil and Natural Gas Sector.

Since the United States imports more petroleum from Canada than any other nation, much of it through pipelines, TSA works closely with our Canadian security counterparts to secure the U.S.-Canadian cross-border pipeline network. TSA and the Canadian National Energy Board coordinate closely on pipeline security matters to include exchanging information on assessment procedures, exercises, and security incidents. Since 2005, TSA and Natural Resources Canada have cosponsored the International Pipeline Security Forum, an annual 2-day conference that enhances the security domain awareness of hazardous liquid and natural gas pipeline operators and provides opportunities for discussion of major domestic and international pipeline security issues. Administrator Neffenger had the pleasure of attending last year's Forum, and enjoyed the opportunity to engage with key industry leaders and learn more about their operations. The Forum presents a unique opportunity for TSA to directly engage with a large number of pipeline industry leaders from the United States and Canada, as well as key government and law enforcement partners. Approximately 160 attendees participate in the annual Forum, including pipeline system owners and operators, pipeline trade associations, U.S. and Canadian government officials, and members of the security, intelligence, and law enforcement communities from the United States, Canada, and other countries.

## SECURITY TRAINING AND GUIDELINES

To assist pipeline owners and operators in securing their systems, TSA developed and distributed security training for industry employees and partners to increase domain awareness and ensure security expertise is widely shared. TSA's pipeline security training products include a security awareness training program highlighting signs of terrorism and each employee's role in reporting suspicious activity, an improvised explosive device awareness video for employees, and an introduction to pipeline security for law enforcement officers.

Additionally, TSA developed the TSA Pipeline Security Guidelines to provide a security structure for pipeline owners and operators to voluntarily use in developing their security plans and programs. The guidelines also serve as a standard for TSA's pipeline security assessments. TSA developed the guidelines with the assistance of industry and Government members of the Pipeline Sector and Government Coordinating Councils, pipeline trade associations, cybersecurity specialists, and other interested parties. Wide-spread implementation of this guidance by the pipeline industry has enhanced critical infrastructure security throughout the country. TSA is currently working with stakeholders to update these guidelines. The guidance has served as a template for entities establishing a corporate security program and has resulted in an increase in the quality of those programs reviewed by TSA. Since the publication of the guidelines, TSA has also seen an increase in the number of pipeline operators conducting security drills and exercises, an increase in coordination with local law enforcement agencies, and an increase in the number of operators conducting security vulnerability assessments of their critical facilities, all of which are recommended in the guidelines.

## EXERCISES, ASSESSMENTS, AND INSPECTIONS

TSA works with industry partners to assess and mitigate vulnerabilities, and improve security through collaborative efforts including exercises, assessments, and inspections. With the support of Congress, TSA developed the Intermodal Security Training and Exercise Program (I–STEP). TSA facilitates I–STEP exercises across all surface modes, including pipelines, to help operators test their security plans, prevention and preparedness capabilities, threat response, and cooperation with first responders. TSA uses a risk-informed process to select the entities that receive I–STEP exercises and updates I–STEP scenarios as new threats emerge to ensure industry partners are prepared to exercise the most appropriate countermeasures.

To identify shortfalls in pipeline security and develop programs and policies to enhance industry security practices, TSA conducts both corporate and physical security reviews with pipeline operators. While these reviews are voluntary, they have been welcomed by pipeline owners and operators who appreciate the value resulting from securing their systems.

Working with key executives and security personnel, TSA conducts the Corporate Security Review (CSR) program, which provides a company-wide assessment of operators' security policies, plans, and programs. Upon completion of each CSR, TSA provides recommendations to the company to enhance its physical and cybersecurity policies and plans. TSA has conducted over 140 CSRs since 2002, including 6 CSRs in fiscal year 2015 and 4 to date in fiscal year 2016, with an additional 4 scheduled for completion by the end of the fiscal year. TSA has completed reviews of all 100 highest-risk pipeline systems and is now conducting return visits to evaluate the implementation status of previous security recommendations.

TSA conducts field-based physical security reviews to assess security measures in place at pipeline critical facilities. The Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53) required TSA to develop and implement a plan for inspecting the critical facilities of the top 100 pipeline systems in the Nation. TSA conducted these required inspections between 2008 and 2011 through the Critical Facility Inspection program and is continuing the effort through TSA's Critical Facility Security Review (CFSR) program. Since 2008, TSA has conducted over 400 physical security reviews of critical facilities, with 46 CFSRs completed in fiscal year 2015 and 21 completed to date in fiscal year 2016, with 16 more expected to be completed by the end of this fiscal year.

## CYBERSECURITY

In the pipeline mode, TSA supports DHS cybersecurity efforts in support of the National Institute of Standards and Technology Cybersecurity Framework. The cybersecurity framework is designed to provide a foundation that industry to better manage and reduce their cyber risk. TSA shares information and resources with its industry stakeholders to support their adoption of the framework. TSA also distributed a cybersecurity toolkit developed from DHS Critical Infrastructure Cyber Community C3 Voluntary Program materials and designed to offer the pipeline industry an array of no-cost resources, recommendations, and security practices. Additionally, within the pipeline industry, TSA is coordinating a voluntary cyber-assessment program with the Federal Energy Regulatory Commission to examine pipeline operators' cybersecurity programs. TSA works closely with the pipeline industry to identify and reduce cybersecurity vulnerabilities, including facilitating Classified briefings to increase industry's awareness of cyber threats.

### CONCLUSION

Through voluntary programs and extensive engagement and collaboration, TSA works closely with Government and industry stakeholders to secure the Nation's pipeline systems from terrorist attacks. TSA shares information with pipeline owners and operators, develops and distributes training materials and security guidelines, conducts security exercises, assessments, and inspections, resulting in an enhanced security posture throughout the pipeline industry. TSA continues to augment its efforts in the face of an evolving threat through the development and implementation of intelligence-driven, risk-based policies and programs. Thank you for the subcommittee's support of TSA's goals and the opportunity to discuss these important issues.

Mr. KATKO. Thank you, Ms. Proctor. I will note that oftentimes we are here to deal with problems related to TSA. But it appears that this program is working remarkably well, and it is reflective of your efforts so we appreciate that.

Now the next witness is Mr. Andrew Black who currently serves as president and CEO of the Association of Oil Pipe Lines. Prior to joining AOPL, Mr. Black served as a director of Federal Government relations at El Paso Energy, where I served long ago as a Federal prosecutor in El Paso back in the 1990s, and deputy staff director for the House Committee on Energy and Commerce. The Chair now recognizes Mr. Black to testify.

## STATEMENT OF ANDREW J. BLACK, PRESIDENT AND CEO, ASSOCIATION OF OIL PIPE LINES

Mr. BLACK. Chairman and Ranking Member, thanks for the invitation. Thanks for your great opening statements, which I thought you captured very well, the program and its benefits.

AOPL represents the owners and operators of the pipelines that bring to American workers and consumers crude oil, refined products like gasoline, diesel fuel, and jet fuel, and natural gas liquids such as propane and ethane. I am also testifying today on behalf of the American Petroleum Institute which represents the broader oil and gas industry, including pipelines. The security of our pipeline systems is a top priority for pipeline operators. We share TSA's goal of pipeline security, and work hard to secure our facilities and networks. Our members appreciate the constructive approach the TSA Pipeline Security Division takes.

Pipeline operators carefully review TSA's pipeline security guidelines and pipeline security smart practice observations when designing and maintaining security plans. Operators host TSA for corporate security reviews and pipeline security inspections, which our members tell us are challenging and pragmatic. Follow-up discussions often result in specific improvements to the operator's security program. We do not today ask for any legislative changes regarding TSA's pipeline security programs.

We participate in the Oil and Natural Gas Sector Coordinating Council and the Pipeline Sector Coordinating Council which provide opportunities for Classified and Unclassified discussions of pipeline security threats. Operators participate in TSA pipeline security stakeholder calls to develop industry-wide awareness of issues seen by TSA and by pipeline operators.

To defend their systems against cyber attacks, pipeline operators follow API standard 1164 for pipeline data security. The standard requires operators to maintain systems for controlling pipeline operations separate and apart from business systems with internet access and helps operators protect systems in a rapidly changing and increasingly complex cyber environment. The broader oil and natural gas industry has also created several information sharing forms, including the oil and natural gas information sharing and analysis center or ONG–ISAC to share threat indicators, alerts, and information to identify emerging cyber threats. API has developed several other standards and programs to promote a culture of security, both physical and cyber, listed in my written testimony.

I want to bring to the subcommittee's attention a pending policy issue of significant security implications. Pipeline operators prepare and submit to the U.S. DOT PHMSA, our safety regulator, oil spill response plans. These response plans contain sensitive security information such as worst-case spill scenarios, first responder operational information, and pipeline control system locations and information. As Members of this subcommittee can appreciate, this information would provide a blueprint for a terrorist attack on pipeline infrastructure.

In 2012, Congress authorized PHMSA specifically to redact this sensitive security information when making response plans public in response to FOIA requests. However, a provision in the recent Pipeline Safety Reauthorization bill passed by the Senate could allow the public to gain access to pipeline security information that terrorists could use to plan an attack.

An amendment adopted in committee would require PHMSA to provide to Congress upon request unredacted copies of oil pipeline response plans. We support Congress exercising its role over PHMSA, its oversight role, and do not object to Congressional committees receiving these plans. Unfortunately, however, as 2276 does not provide clear or specific protections against public disclosure of security sensitive response plan information obtained by Congress.

PHMSA has explained this information, "if disclosed would be of significant operational utility to a person seeking to harm the pipeline infrastructure of the U.S." Like PHMSA, we believe this information must be protected from public disclosure because of the security risks. We are ready to discuss this with this and other committees as pipeline safety legislation moves forward.

Finally, there is a growing pipeline security issue that operators are watching closely. Opponents to pipeline projects in Canada are breaking into pipeline facilities, tampering with valves, and locking themselves to equipment as part of theirs protests. There were 4 recent incidents on 1 pipeline, and a fifth on another. These actions could harm an operator's ability to respond to an incident. Could even unintentionally result in a pipeline release impacting the public and the environment. Information from unredacted response plans may have helped some Canadian protestors in choosing where and how to obstruct a pipeline's activities. Information circulated for, or by pipeline opponents, can easily reach terrorist organizations who might intentionally use this information to harm the public.

I encourage Congress to keep these new threats in mind when reviewing unredacted response plans and determining how the important information within them should be withheld from public disclosure.

I thank the subcommittee for considering these issues and be happy to respond to any questions.

[The prepared statement of Mr. Black follows:]

## PREPARED STATEMENT OF ANDREW J. BLACK

APRIL 19, 2016

Thank you for holding this hearing and for inviting me to testify.

I am Andy Black, president and CEO of the Association of Oil Pipe Lines (AOPL). AOPL represents the owners and operators of pipelines that transport crude oil, refined products like gasoline, diesel fuel, and jet fuel, and natural gas liquids like propane and ethane, to American workers and consumers.

I am also testifying today on behalf of the American Petroleum Institute (API). API represents all facets of the oil and natural gas industry, with more than 650 members including large integrated companies, as well as exploration and production, refining, marketing, pipeline, and marine businesses, and service and supply firms.

### PIPELINE SECURITY AND TSA

The oil and natural gas industry is committed to achieving zero incidents throughout our operations. Pipeline operators take considerable steps to ensure the safety and security of our personnel, assets, and operations. The security of our pipeline systems is a top priority for pipeline operators. Liquid pipeline operators share TSA's goal of pipeline security, and work hard to secure our facilities and networks. Pipeline operators implement many measures and programs in pursuit of our goal of zero incidents. Operators assess threats to pipelines, including security threats, take steps to address them, and share pipeline security best practices industry-wide.

AOPL and API members appreciate the constructive approach the TSA Pipeline Security Division takes with its pipeline security program. Pipeline operators carefully review TSA's *Pipeline Security Guidelines* and *Pipeline Security Smart Practice Observations* when designing and maintaining security plans. Pipeline operators host TSA for pipeline security inspections and Corporate Security Reviews, which our members tell us are challenging, reasonable, and pragmatic. Follow-up discussions often result in specific improvements to the operator's security program. We do not ask for any changes in legislation or regulations regarding TSA's programs and activities in pipeline security.

Because of the pipeline industry's designation by the Department of Homeland Security (DHS) as a critical infrastructure subsector, we have many opportunities to participate in Government programs focusing on promoting security and identifying threats. We participate in the DHS Oil and Natural Gas Sector Coordinating Council established under Presidential Policy Directive 21 on critical infrastructure security and resilience. These activities provide important opportunities for both Classified and Unclassified discussions of pipeline security threats. In addition, pipeline operators participate in the DHS Regional Resiliency Assessment Program, and regularly participate in TSA pipeline security stakeholder calls to develop industry-wide awareness of issues seen by TSA and by operators. We also participate in the FBI's Infragard process, a Government-industry partnership dedicated to sharing information and intelligence to prevent hostile acts against the United States.

While participation in these efforts is critical to the development of situational awareness, it should be noted that DHS's risk analysis of all critical infrastructure did not designate any oil or natural gas infrastructure into its highest tier of risk. This is due to our industry's diverse geography, redundant systems, and the resilience of the sector when responding to events.

### CYBERSECURITY AND API STANDARD 1164

Pipeline operators follow API Standard 1164, *Pipeline SCADA Security*, which helps pipeline operators defend their systems from cyber attacks. The standard requires operators to maintain systems for controlling pipeline operations separate and apart from business systems with internet access. It was developed with a broad group of stakeholders from the public and private sectors, and helps operators protect systems in a rapidly changing and increasingly complex cyber environment.

The broader oil and gas industry, including pipeline owners and operators, have also created several information sharing forums, including the Oil and Natural Gas Information Sharing and Analysis Center (ONG ISAC), to share threat indicators, alerts and information to identify emerging cyber threats. Pipeline operators also participate in the NIST Cybersecurity Framework Roadmap process. These efforts, combined with the intelligence and information operators receive from Government sources, help operators better understand their risk and prevent incidents.

### OTHER INDUSTRY PIPELINE SECURITY PROGRAMS

API has also developed several other standards and programs to promote a culture of security, both physical and cyber. API RP 780, *Security Risk Assessment*, defines the recommended approach for assessing security risk widely applicable to the types of facilities operated by the industry and the security issues the industry faces. API RP 781, *Facility Security Plan Methodology for the Oil and Natural Gas Industries*, will build on RP 780 and provides the process to factor risk assessment into the physical and cybersecurity measures used to secure operations. This recommended practice should be published later this year. In addition, API has published *Utilizing Intelligence to Secure People [http://www.api.org//media/files/policy/safety/api-guidance-utilizing-intelligence-in-ong.pdf?la=en],* a guidance document describing some of the resources that are available to the industry to help attain situational awareness in different operating environments.

API created the *Oil and Natural Gas Industry Preparedness Handbook [http://www.api.org/news-policy-and-issues/safety-and-system-integrity/oil-gas-industry-preparedness-handbook]* with support from members and associations throughout the industry, to illustrate how local responses can be aided by established relationships with governments and communities, local, State, and regional associations, and how corporate and Federal capabilities can facilitate efficient response and recovery at the local level. The Handbook provides a common-sense approach for oil and gas owners and operators, local and State industry associations, and public-sector partners to build the necessary capabilities to effectively manage the information flow that so often becomes congested during disruptive events.

### OIL SPILL RESPONSE PLANS

I want to bring to the subcommittee's attention a pending pipeline policy issue with significant security implications. Pipeline operators prepare and submit to U.S. DOT PHMSA, our safety regulator, oil spill response plans. These response plans detail facilities and plans for first responder and operator response to pipeline emergencies. They contain sensitive security information, such as worst-case spill scenarios, first responder operational information, pipeline control system locations and information, and descriptions of high-consequence areas. As Members of this subcommittee can appreciate, this information would provide a blueprint for a terrorist attack on pipeline infrastructure.

In 2012, Congress authorized PHMSA specifically to redact this sensitive security information when making oil spill response plans public in response to Freedom of Information Act requests. However, a provision in the recent pipeline safety program reauthorization bill, S. 2276, passed by the Senate earlier this year, could allow the public to gain access to pipeline security information terrorists could use to plan an attack.

The specific Senate provision, adopted in committee as an amendment by Senator Markey, would require PHMSA to provide to Congress, upon request, unredacted copies of oil pipeline response plans. AOPL and API support Congress exercising its oversight role over PHMSA and the oil spill response program, and do not object to Congressional committee leaders receiving these plans. Unfortunately, however, S. 2276 does not provide clear or specific protections against public disclosure of security-sensitive oil spill response plan information obtained by Congress.

PHMSA legal guidance deems the information at issue here, "if disclosed, would be of significant operational utility to a person seeking to harm the pipeline infrastructure of the U.S." Like PHMSA, we believe this information must be protected from public disclosure because of these security risks. We are ready to discuss this with you and with Members of this committee, the Transportation and Infrastructure Committee, and the Energy and Commerce Committee, as pipeline safety reauthorization legislation moves through the House and conference in coming months.

### NEW THREATS AND ACTIONS AGAINST PIPELINES

Finally, there is a growing pipeline security issue operators are watching closely. Opponents to pipeline projects in Canada are breaking into pipeline facilities, tampering with valves, and locking themselves to equipment as part of their protests. There were 4 incidents[1] between November and January on 1 pipeline and a fifth incident[2] on another in January. These actions could harm a pipeline operator's ability to respond to an incident and could even unintentionally result in a pipeline release impacting the public or environment.

I understand information from unredacted oil spill response plans has helped some Canadian protestors in choosing where and how to obstruct a pipeline's activities. Information circulated for, or by, pipeline opponents can easily reach terrorist organizations who might intentionally use this information to harm the public. I encourage Congress to keep these new threats in mind when reviewing unredacted response plans and determining how the important information within them should be withheld from public disclosure.

I thank the subcommittee for considering these issues, and would be happy to respond to any questions.

Mr. KATKO. Thank you, Mr. Black.

Our third witness is Ms. Kathleen Judge, who currently serves as a director of risk and compliance for global security at National Grid, which I am proud to say operates in my hometown of Syracuse and throughout up-State New York. Ms. Judge also serves as the chair of the Oil and Natural Gas Sector Coordinating Council. The Chair now recognizes Ms. Judge to testify.

## STATEMENT OF KATHLEEN S. JUDGE, DIRECTOR OF RISK AND COMPLIANCE FOR GLOBAL SECURITY, NATIONAL GRID, TESTIFYING ON BEHALF OF THE AMERICAN GAS ASSOCIATION

Ms. JUDGE. Chairman Katko, Ranking Member Rice, Members of the committee, thank you the opportunity to provide testimony on pipeline security, and your commitment to the security of our Nation's critical infrastructure.

As the Chairman stated, I am Kathy Judge. I work for National Grid, which is a gas and electric company based in the United Kingdom and Northeastern United States that serves nearly 7 million customers in New York, Massachusetts, and Rhode Island. National Grid is the largest distributor of natural gas in the Northeast. We are proud to be the energy provider to the Chair, Ranking Member, and Representative Keating's district.

My background includes 27 years in the utility industry. Relevant to this hearing, I have helped lead the American Gas Association Security Committee. I also am current chair of the Oil and Natural Gas Sector Coordinating Council and Pipeline Sector Coordinating Council.

Today I am testifying on behalf of the American Gas Association which represents more than 200 local gas utilities that operate 2½ million miles of distribution pipelines that deliver gas to 71 million consumers. Providing safe natural gas delivery is the top priority

---

[1] "Pipeline industry concerned about tampering and vandalism", *CBC News,* March 9, 2016, *http://www.cbc.ca/news/business/cepa-chris-bloomer-pipelines-tampering-enbridge-vandalism-target-1.3480857.*

[2] "Pipeline sabotage: Someone tampered with valve on Enbridge fuel pipeline near Cambridge", *Hamilton Spectator,* January 5, 2016, *http://www.thespec.com/news-story/6219719-pipeline-sabotage-someone-tampered-with-valve-on-enbridge-fuel-pipeline-near-cambridge/.*

for natural gas utilities. This said, here are some important facts about pipeline security.

One, natural gas utilities have a proven history of weathering natural disasters, accidental third-party damage, and intentional assaults. Ironically, the leading risk to pipelines is third-party excavation damage. Pipeline systems are resilient with multiple redundant safety and reliability mechanisms in place. Pipelines must comply with DOT pipeline safety regulations that also provide some security coverage.

TSA threat assessments have indicated that the threat against U.S. natural gas pipelines is low. Nevertheless, because of the impact a successful physical or cyber attack could have on millions of customers, pipeline security remains a top industry priority.

Gas utilities employ numerous strategies to ensure pipeline security, including but not limited to, site-specific security and crisis management plans, to ensure operations are reinforced with workplace and system redundancies, embedding security requirements into pipeline design and construction, weaving security requirements into corporate governance, participating with information sharing and analysis centers to improve on situational awareness, coordinating with Federal, State, and local first responders to ensure effective incident prevention and response, and partnering with Federal security partners at TSA, DOE, and the FBI to better understand the potential threats.

Pivotal to pipeline security is the partnership industry has, with TSA's pipeline section of the Office of Security Policy and Industry Engagement. The TSA pipeline section recognized early on that collaboration was key because pipeline security professionals in TSA share the same objective, to protect critical infrastructure. Fourteen years later, this approach serves as a model for the public/private partnership. To sustain that partnership, TSA offers numerous programs to aid pipeline operators. Those primary tools are the TSA pipeline security guidelines which are a flexible set of security smart practices that were developed collaboratively by the Federal Government and pipeline security professionals. On-site security reviews which offer TSA the opportunity to engage in constructive nonregulatory discussions with pipeline operators, and they also offer security awareness and training materials. These programs promote security in mutually beneficial relationships between TSA and the operator cannot be undervalued. Please note that the TSA pipeline security program must be protected.

I would like to share 2 examples of past actions taken with the best of intentions that proved detrimental. In 2014 TSA announced the significant organizational realignment that dismantled the effective programs and processes that were in place and that we benefitted from as operators. During this realignment, it was the intent of DHS to have generalists. In other words, GSA reps who worked across all transportation modes. This proved ineffective as visits focused more on educating the generalists about pipelines and pipeline security than on the bilateral value gained from the prior visits with specialists. After input from pipeline operators and a decline in the industry engagement, TSA reversed the realignment and went back to the way it was.

DOT and TSA security partnership needs greater collaboration. DOT recently proposed changes to its National pipeline mapping system that would require operators to provide on-line, in a single database, detailed pipeline operations' location information. It is my belief that TSA would have opposed this had they been collaborated with on this subject.

Natural gas utilities value the effective security partnership. Compliance does not equal security. The formula for measurable effectiveness of TSA's pipeline program is a result of practical guidelines, information exchange, and trusted private-sector engagements. We also urge the committee to continue to support the TSA pipeline security program and encourage interagency collaboration with PHMSA where pipeline security and pipeline safety overlap.

Thank you. I look forward to your questions.

[The prepared statement of Ms. Judge follows:]

## PREPARED STATEMENT OF KATHLEEN S. JUDGE

APRIL 19, 2016

My name is Kathleen S. Judge and I am the director, risk & compliance, corporate security for National Grid. National Grid is an international electricity and gas company based in the United Kingdom and northeastern United States that connects nearly 7 million customers to vital energy sources through its networks in New York, Massachusetts, and Rhode Island. It is the largest distributor of natural gas in the Northeast. National Grid also operates the systems that deliver gas and electricity across Great Britain.

I have over 27 years of experience in the utility industry, and since 2007, I have been in physical security. I have been actively involved with the industry trade association security committees during my time in security, including serving on the American Gas Association Security Committee leadership team since 2011. I currently chair the Oil & Natural Gas Sector Coordinating Council (ONG SCC) and Pipeline Working Group, which also serves as the Pipeline Sector Coordinating Council. I am also actively involved in the Edison Electric Institute (EEI) Security Committee and serve on the Executive Steering Committee for the Long Island Sound Area Maritime Security Committee. In 2014 and 2015, I was an active member on the NERC CIP 14—Physical Security Standards Drafting Team.

I am testifying today on behalf of the American Gas Association (AGA). AGA, founded in 1918, represents more than 200 local energy companies that deliver clean natural gas throughout the United States. There are more than 72 million residential, commercial, and industrial natural gas customers in the United States, of which 95 percent—nearly 69 million customers—receive their gas from AGA members. Natural gas pipelines, which transport approximately one-fourth of the energy consumed in the United States, are an essential part of the Nation's infrastructure. Indeed, natural gas is delivered to customers through a safe, 2.5 million-mile underground pipeline system. This includes 2.2 million miles of local utility distribution pipelines and 300,000 miles of transmission pipelines that stretch across the country, providing service to more than 177 million Americans.

### NATURAL GAS UTILITIES

### *Who We Are*

Providing safe, reliable, and cost-effective delivery of natural gas is the top priority of natural gas utilities across America. Given our strong service record, enviable safety statistics, and inherently resilient makeup due to the subsurface locations of the majority of our assets, natural gas utilities work vigilantly to maintain both the cybersecurity and physical security of the infrastructure. The natural gas system is a complex, interconnected, and well-protected network of pipelines and associated facilities, including but not limited to, compressor stations, pressure regulators, pressure relief valves, and underground natural gas storage. Natural gas operations have a proven history of weathering natural events, accidental third-party damage, and intentional malicious assaults. Crisis management and site-specific security plans ensure operations are reinforced with well-trained workforce and system redundancies. Natural gas security professionals layer security measures within a framework of risk management. Further, natural gas owner/operators partner with Federal, State, and local government and law enforcement agencies to ensure effective and efficient response to events impacting natural gas operations.

The Transportation Security Administration (TSA) annual threat assessments have indicated that the threat against U.S. natural gas pipelines is low, and there is no current credible threat information regarding attacks on U.S. distribution pipelines. Further, the U.S. Department of Transportation (DOT) Bureau of Transportation Statistics continue to show pipelines as the safest form of transportation with very low incident rates, and the DOT Pipeline and Hazardous Materials Safety Administration (PHMSA), which regulates pipelines under its Office of Pipeline Safety (OPS), states that pipelines are one of the safest and most cost-effective means to transport the extraordinary volumes of natural gas. As such, pipeline safety and physical infrastructure security remain AGA's top priority.

### *Pipeline Risks*

The primary objective for gas utilities is the safe and reliable delivery of natural gas to the consumer. As a result, natural gas utilities evaluate their security risks with public safety and natural gas interdependencies in mind. Pipeline security risks may be categorized as physical security risks or cybersecurity risks. In general, the leading security risks to natural gas utilities include, gas theft; access control; supply chain integrity; customer information theft; insider threat; facility and employee protection; and breach of Supervisory Control And Data Acquisition systems (SCADA), control systems, or communication systems. In addition, the potential for loss of telecommunications capability motivates the natural gas industry to maintain a basic level of manual operations, which adds a layer of security not afforded sectors that are fully automated.

Ironically, the leading risk to natural gas utility pipelines continues to be third-party excavation damage. Excavation damage causes more casualties and service interruptions than any combination of security incidents.

While specifics may vary across companies, natural gas security professionals layer security measures in a handful of operational phases, i.e., planning, preparation, protection, incident response, and recovery that are framed by the overarching goal of risk management. The following provides more details about the activities associated with these phases.

- *Planning*.—Natural gas owner/operators develop written programs that include methods for vulnerability and risk assessment, protection of sensitive information, threat responses, cooperation with public safety personnel, and physical security and cybersecurity practices.
- *Preparation Activities*.—Natural gas owner/operators practice and prepare for extraordinary scenarios through participation in their own drills as well as those coordinated by industry, regional associations, and Government agencies. Table-top exercises enhance preparedness efforts and incident classification, while testing and engaging operators in restoration and recovery discussions. Finally, the industry participates in the TSA I–STEP[1] full-scale training and exercises designed to provide a forum for personnel to practice specific plans and procedures in response to security issues impacting their companies.
- *Protection Strategies*.—Natural gas owner/operators make significant investments to protect their most critical assets. These investments focus on improving protection, detection, and perimeter security at the most critical locations. Examples of enhanced physical and personnel security measures include:
  - physical security measures such as, but not limited to and as appropriate, barriers and buffer zones, access controls, gates, locks and key controls, facility lighting, vehicle searches (static guards), surveillance cameras, intrusion detection, and monitoring.
  - personnel security measures such as, but not limited to and as appropriate, biometric identification and badging, background investigation, training, exercises, and drills.
- *Incident Response and Recovery*.—Gas utilities have long maintained and been acknowledged for their consistent commitment to the safety of the natural gas infrastructure, workers, and processes. The commitment to operational resiliency is equally substantial. Redundancies along the delivery system provide operators the flexibility to reduce pressure and redirect, shut down, or restore gas flow. Facilities for alternative fuels and natural gas storage provide additional options to supplement gas supply to minimize service disruption. Companies

---

[1] I–STEP: The Intermodal Security Training & Exercise Program is a "risk-based, intelligence-driven exercise, training, and security planning solution in collaboration with other security partners to reduce risks to critical transportation infrastructure, and build and sustain security preparedness."

also have critical back-up and replacement equipment and parts stored at key points along a system. Rapid response teams can be quickly deployed to get the system up and running in order to reduce down time. Overall, the industry approaches preparedness and response from the local level, acknowledging that events impact workers, businesses, and communities first and foremost. While resources and information are often held at the regional or National levels, it is the local facility operators who have the best ability to assess their systems, identify needs, and execute the work needed to restore services.

Title 49 of the Code of Federal Regulations governs the response aspect of security planning. Pipeline companies have years of experience responding to emergency incidents and are required by DOT to have effective emergency plans in place. Operators are also required to report significant incidents—those resulting in serious injury, loss of life, or property damage greater than $50,000—to the DOT National Response Center (NRC). A mechanical failure or unintentional act resulting in significant damage to a pipeline will be reported to DOT through the NRC. An intentional act of damage, or act of a suspicious nature involving a pipeline, will be reported to TSA through the Transportation Security Operating Center (TSOC).

Responding to a pipeline failure caused by an intentional act varies little from the response to a mechanical failure or an unintentional act; except that, operators must exercise caution recognizing the incident may be criminal in nature. Facility restoration is the final component of an industry security initiative. Specific plans will vary among operators based on the criticality of the pipelines and factors such as location and time of year.

Security is woven into corporate governance through security policies, incident procedures, record keeping, communication, security measures embedded within design and construction practices, as well as equipment maintenance and testing. To help maintain operational security, natural gas utilities are careful not to publicize clearly sensitive information about critical infrastructure that might provoke new threats, or endanger the safety of the American public or the integrity of the Nation's gas systems. Gas companies work closely with law enforcement personnel and first responders on site-specific security plans and security drills. Additionally, gas utilities participate in security information-sharing communities such as the Downstream Natural Gas Information Sharing & Analysis Center, which provides participants with timely situational awareness, intelligence analytics, and industry incident information exchange.

*Sector Coordinating Council*

In 2004, Sector Coordinating Councils were formed to coordinate security initiatives among the Nation's critical infrastructure assets. The Oil and Natural Gas Sector Coordinating Council (ONG SCC) was formed by 19 industry trade associations to provide a forum for discussion and to coordinate communications between industry security professionals and representatives of the Energy Sector Government Coordinating Council (Energy GCC[2]). Subsequent to the formation of the ONG SCC, the Pipeline Working Group (Pipeline Sector Coordinating Council) was formed to further enhance communication and collaboration among pipeline operators and Government entities.

*Cooperation*

The pipeline industry takes its responsibility for facility, system, and network security very seriously. The TSA provides guidance and expectations for the practices and procedures necessary to secure the Nation's critical pipeline infrastructure. Members of industry and trade associations, working together and through the SCCs, have developed guidelines that are consistent with these expectations. The typical operator has a developed security program, has conducted facility risk assessments, and has implemented sound practices that provide for effective and practical system security.

The natural gas industry supports a process for raising public awareness about pipelines in a manner that does not jeopardize security, interstate commerce, or proprietary business information. In addition to close coordination amongst gas utilities to reinforce operational resilience, the industry works directly with Government partners in DHS, DOE, the White House, the Government intelligence community, and local and State law enforcement agencies to more thoroughly understand potential threats and to better protect its systems. AGA and gas industry representatives

---

[2] Energy GCC: The Energy Sector Government Coordinating Council is chaired by a representative of the Department of Energy, and the GCC includes members of numerous agencies, including TSA and DOT.

actively participate in interdependency initiatives coordinated by Federal and State governments to enhance preparedness, response, and recovery planning. For example, in 2010 and in support of the objectives of the National Infrastructure Protection Plan, owner/operators across the oil and natural gas sector collaborated with DHS and DOE to present several cross-sector emergency management workshops aimed at promoting an integrated private sector and Government response during natural disasters and terrorist incidents. The gas industry also engaged with DOE, DHS, electric utility operators, and local law enforcement on a series of physical security and cybersecurity briefings across the United States and Canada. These briefings allow Government officials to provide information on the current threat environment, discuss mitigation strategies, and encourage participants to further develop relationships with first responders and industry partners. Additionally, many utility security personnel hold Government security clearances, which allow access to Classified threat information to further develop security strategies.

### *Resilience*

Resilience is an integral element of the gas industry's critical infrastructure protection mission that is bolstered by multiple layers of safety and reliability mechanisms to reduce the magnitude and/or duration of disruptive events and to ensure sufficient backup coverage exists. Because utilities must "expect the unexpected," they have all-encompassing contingency plans for dealing with man-made and natural disasters to help ensure natural gas will flow safely and reliably. The industry continues to work with Federal agencies to enhance the physical security and cybersecurity of its critical infrastructure while remaining firmly committed to taking appropriate and measured actions to deter threats, mitigate vulnerabilities, and minimize consequences associated with a terrorist attack and other disasters.

The National Infrastructure Advisory Council's *Critical Infrastructure Resilience Study* found that the oil and natural gas sector has a significant amount of redundancy and robustness built into the system. Most pipelines are relatively easy to repair over the short term and in many cases, alternative routes are also available to move sufficient amounts of product around the site of an incident, thus preventing major disruptions. Moreover, redundancies are built into the pipeline infrastructure, including interconnects between companies. This planning and interconnect capability ensures consumers with reliable service.

## TRANSPORTATION SECURITY ADMINISTRATION

### *Pipeline Security Authority*

Under the provisions of the Aviation and Transportation Security Act (Public Law 107–71), TSA was established on November 19, 2001, with responsibility for civil aviation security and "security responsibilities over other modes of transportation that are exercised by the Department of Transportation." To fulfill this mandate in the pipeline mode, on September 8, 2002, TSA formed the Pipeline Security Division, which is now called the Pipeline Section of the Office of Security Policy and Industry Engagement (TSA Pipeline Section).

### *Partnership*

The vast majority of critical infrastructure is privately owned and operated. As such, effective public-private partnerships are the foundation for critical infrastructure protection and resilience strategies comprising timely, trusted, unguarded information sharing among stakeholders. The TSA Pipeline Section recognized early on that the pipeline industry security professionals are charged with a parallel objective, i.e., protect the critical infrastructure, and this is best accomplished in a collaborative environment. Historically, TSA has strategically refrained from executing its regulatory authority and, instead, pioneered a path of genuine Government partnership with pipeline owners/operators. Fourteen years later, this approach continues to serve as a model for public/private partnership that offers collaboration, mutual support, and measurable achievement towards a common goal—pipeline security.

The partnership approach has established a bond between industry and Government that is uncommon across the Government/operator community and is measurably beneficial for all stakeholders. The operator knows best his/her operations—what needs to be secured and how to best achieve this; TSA provides valuable tools, knowledge resources, insights, and perspectives that advances the operator's decision-making process. The end result is an improved security posture that benefits all involved, except the adversary.

### *Programs / Tools / Products*

TSA has many programs, tools, and products available to assist pipeline operators in addressing security matters. The portfolio includes, Critical Facility Inspections (CFI), Corporate Security Reviews (CSR), Critical Facility Security Reviews (CFSR), Blast Mitigation, Smart Practices, I–STEP, monthly stakeholder teleconferences, Security Awareness Training Videos, and the International Pipeline Security Forum. These resources bring Government and operators together and foster relationships and cooperative efforts that have been key to advancing industry pipeline security practices.

#### *TSA Pipeline Security Guidelines*

The leading tool in the TSA portfolio is the TSA Pipeline Security Guidelines (*Guidelines*), a product of collaboration that coalesced the institutional knowledge and experience of pipeline security professionals with the resources of the Federal Government. The *Guidelines* were developed with the assistance of industry and Government members of the Pipeline Sector and Government Coordinating Councils, industry association representatives, and other interested parties and represent TSA's expectations of industry. TSA released the *Guidelines* in December 2010 (re-released in April 2011), and it applies to natural gas distribution pipelines and liquefied natural gas facilities. Notably, the partnership between pipelines and TSA effectively drives industry to advance beyond minimum security standards to the deployment of smart industry practices. The *Guidelines* provides operators the flexibility to secure pipeline infrastructure by applying practices that are most applicable to their individual systems.

#### *On-site Reviews / Visits*

Equally significant in advancing industry's security posture are non-regulatory, on-site facility reviews/visits. The CSRs and CFIs have historically been the program names for these reviews/visits conducted by the TSA Pipeline Section. The CSRs focused on the operators' overall security plan. The CFIs focused on security plan implementation and actual day-to-day security practices at critical facilities. More recently, CFIs have been renamed as CFSRs.

The CSRs are designed for TSA to focus on an operator's overall security plan implementation through: (1) Learning more about an organization's pipeline system, (2) reviewing an organization's listing of critical facilities, (3) discussing at length the details of an organization's security plan and programs, and (4) engaging with the operator to familiarize the operator with TSA and vice-versa prior to any security-related event or emergency. Following the review, TSA shares observations with that company, including a security benchmark so the company can compare itself with similar or peer companies. TSA discusses areas in which they observe the company excelling in relation to the industry and smart practices. TSA also identifies areas in which the company is observed to be lacking and will make recommendations based on the *Guidelines* or offer considerations based on their expertise and industry observations. TSA then follows up with each organization to see what progress has been made based on their recommendations.

CFSRs are site-by-site walkthroughs at each critical facility focused on site-specific security plans and measures. Following each review, TSA sends a report to the operator including commendations and recommendations. TSA then follows up with each operator to check in on the progress of recommendations. TSA also utilizes information obtained during the reviews to develop security smart practices that are shared with the industry.

The review/visits offer TSA a unique opportunity to engage in open, candid, non-punitive discussions with the operator. This affords TSA with a more holistic view of how the industry can be effective in its flexible use of the *Guidelines* and reinforces the fact that constructive exchange between TSA and the operator is more useful for security planning than the "us versus them" compliance-audit environment. Results of these reviews have been used to develop security "smart practices" that are shared widely throughout the industry. These programs have not only been a means of evaluating the actual security practices of the pipeline operators but have also been a means of promoting industry familiarity with the responsibilities and personnel of TSA. Thus, the collaboration between TSA and the pipeline operator is a mutually beneficial relationship that cannot be undervalued.

#### *Stakeholder Teleconferences*

For wider participation, TSA holds monthly stakeholder calls to share physical and cyber threat and intelligence information with industry. Following notable security events, TSA conducts more frequent calls and sends out relevant information to industry stakeholders.

### *Additional Engagement Opportunities*

Industry and TSA annually convene to go through the Transportation Sector Security Risk Assessment. This exercise includes evaluating a list of scenarios and determining the likelihood of such an event. Both also collaborate on the development of Pipeline Modal Threat Assessment prepared by the TSA Office of Intelligence and Analysis.

In addition to the *Guidelines* and TSA products, the pipeline industry references and implements multiple resources, programs, and standards from wellhead to the meter as appropriate for the company's operations. Such resources include American Petroleum Institute Recommended Practices and standards, DOE Oil & Natural Gas Cybersecurity Capability Maturity Model, SANS Institute cybersecurity standards, and the North American Electric Reliability Corporation Critical Infrastructure Protection Committee standards. The pipeline industry also coordinates initiatives with other critical infrastructure sectors, including but not limited to Chemical, Energy, Communications, and Financial Sectors as well as other modes within the Transportation Sector.

### *To Regulate or Not To Regulate*

The formula that promotes on-going improvements to the pipeline industry's security posture consists of the partnership, the *Guidelines*, and the operator facility visits by TSA.

The *Guidelines* has a common goal with the pipeline operator to promote the security pipeline infrastructure while recognizing operational, structural, and commodity differences across the pipeline industry. This performance-based approach supports the flexibility needed for operators to address the dynamic security threats specific to their operations in different operating settings.

The CSRs, CFIs, and CFSRs demonstrate the owner/operators' actions to follow the *Guidelines*. According to TSA, there have been 347 CFIs, 154 CSRs, and 151 CFSRs to date. Each of the visits resulted in TSA recommendations to the operator to which 85–90% of the recommendations have already been addressed by the operator, and the remaining recommendations are in the process of being addressed, or the operator found a better way of achieving the objective of the recommendation. TSA has gone on record stating that based on its CSRs and other information, pipeline operators already employ most of these recommendations in their security plans and programs.

In addition to partnering with TSA, pipelines must comply with DOT pipeline safety regulations, which require the incorporation of system fail-safes that in many cases protect against the goals of the adversary; in the case of natural gas utilities, this would apply to system over-pressurization. Intrastate pipeline must also comply with State pipeline safety regulations that go above and beyond DOT's regulations.

### *Improving on TSA's Role*

In January 2014, TSA announced a significant organizational realignment that dismantled effective programs (previously highlighted) and processes both the Government and the operators had benefited from. During the realignment, it was the intent of DHS to have generalists (i.e., TSA representatives who work all transportation modes) to conduct the CFSRs. In practice, this proved ineffective as the visits focused more on educating the TSA generalist about pipeline security than on bilateral value gained. Ostensibly, the impetus for the realignment was to sustain TSA's effectiveness and to remove the stove-piping amongst the various modes. Industry representatives expressed concern over the reorganization, as this realignment was done without engagement of the operator community.

AGA worked with Congressional staff and TSA staff to facilitate a meeting between TSA leadership and industry to discuss the reorganization. After extensive pressure from pipeline operators and a measurable decline in TSA's engagement with industry, TSA reversed the realignment and returned to a model similar to the original. Because most of the original well-trained TSA pipeline staff had been reassigned elsewhere, the program is slowly rebuilding. AGA credits the leadership of Ms. Sonya Proctor, director, surface division, office of security policy and industry engagement, for recognizing the ineffectiveness of the realignment, the need to return to the original model, and the need to fill open pipeline security positions with qualified candidates. TSA is strongly encouraged to ramp up the CFSR program with reviewers who already understand pipeline operations, as was the case prior to the realignment efforts.

Further, industry has invested a great deal of resources working with the Government intelligence community to ensure the timely sharing of actionable information. Though certain groups, such as DHS Industrial Control Systems Cyber Emergency Response Team (ICS–CERT), recognize the value of this, others within the intelligence community (outside of DHS) do not necessarily agree. TSA should be positioned and empowered to be a conduit of threat information that has implications to pipeline operations. This would include information that could impact sectors/infrastructure upon which pipeline operations are dependent or which have operations similar to pipelines, e.g., SCADA. Along these same lines, more Government resources should be invested to provide well-trained and -equipped pipeline security professionals across the Nation to conduct more facility reviews and noncompliance visits.

### PHMSA

Security and safety go hand-in-hand. As prescribed in Title 49 of the Code of Federal Regulations, pipeline safety, including emergency management, has been the purview of DOT through PHMSA's Office of Pipeline Safety. Prior to events of September 11, 2001, the Homeland Security Act of 2002, Homeland Security Presidential Directive 7 (December 17, 2003), and the Aviation & Transportation Security Act of 2001, pipeline security was under the purview of DOT, where it played a less prominent role than pipeline safety. In September of 2004, a Memorandum of Understanding (MOU) was signed by representatives of DHS and DOT memorializing an agreement of respective pipeline security roles and responsibilities; "DOT and DHS will collaborate in regulating the transportation of hazardous materials by all modes (including pipelines)." Additionally, in August 2006, an MOU was signed by TSA and PHMSA to clarify that TSA has primary responsibility for pipeline security and formalize coordination between TSA and PHMSA to ensure that pipeline security and pipeline safety complement one another: "PHMSA is responsible for administering a National program of safety in natural gas and hazardous liquid pipeline transportation including identifying pipeline safety concerns and developing uniform safety standards."

The emergency response practices prescribed by DOT are used in the event of any incident, whether intentional or accidental. All involved parties must work cooperatively with law enforcement, local agencies, and first responders to minimize damage and danger to local communities and critical facilities.

#### *Coordination*

For a number of years following the 2006 MOU, PHMSA was actively engaged with TSA activities, including the development of the *Guidelines*. However, more recent experiences suggest that PHMSA has lost its focus on cybersecurity. For example, PHMSA has proposed significant changes to its National Pipeline Mapping System that would require operators to provide very detailed pipeline operations and location information, including information on critical valves, on-line in a single database, and this information would be made widely available. PHMSA's actions suggest pipeline cybersecurity is an afterthought rather than part of the evaluation process.

### SUMMARY

Natural gas utilities value the collaborative security relationship they have with TSA. TSA is to be commended for choosing the more constructive path, i.e., partnering with owners/operators, to improving the pipeline sector's security posture. Furthermore, compliance does not equate to security. The formula for the measurable effectiveness of TSA is the result of practical guidelines, smart practices, information exchange, and trusted engagement with the private sector. TSA should continue the process of reversing its earlier realignment efforts and return to the model of a dedicated group of TSA staff with knowledge and experience in pipeline operations specifically assigned to pipeline security. TSA should also continue to coordinate with PHMSA where pipeline security and pipeline safety overlap. Along the same lines, PHMSA should be more proactive in consulting with TSA on pipeline safety matters, in particular regarding regulations that have security implications and may increase pipeline vulnerability.

Mr. KATKO. Thank you, Ms. Judge for your testimony. We appreciate you being here today.

Our fourth and final witness is Dr. Paul Parfomak. Did I say that correctly?

Mr. PARFOMAK. Perfect.

Mr. KATKO [continuing]. Who currently serves as a specialist in the energy and infrastructure policy at the Congressional Research Service. The Chair now recognizes Dr. Parfomak to testify.

## STATEMENT OF PAUL W. PARFOMAK, SPECIALIST IN ENERGY AND INFRASTRUCTURE POLICY, CONGRESSIONAL RESEARCH SERVICE, LIBRARY OF CONGRESS

Mr. PARFOMAK. Good afternoon, Chairman Katko, Ranking Member Rice, and Members of the subcommittee. My name is Paul Parfomak, specialist in energy and infrastructure policy at the Congressional Research Service. CRS appreciates the opportunity to testify about the Federal role in pipeline security. Please note that CRS does not advocate policy or take a position on any legislation.

Nearly 3 million miles of pipeline transport natural gas, oil, and other hazardous liquids across the continental United States. Due to their scale and reliance on computer controls, the Nation's pipelines are vulnerable to attack, and repeatedly have been a focus of malicious activity. Major incidents include a plot by Islamist terrorists to attack jet fuel pipelines at JFK Airport, attempted bombings of natural gas pipelines in Texas and Oklahoma, and a coordinated campaign of cyber intrusions among pipeline operator computer systems.

Over the last 15 years, there have been no successful pipeline attacks in the United States. But the threat remains credible. The Department of Transportation has statutory authority to regulate pipeline safety. The Clinton administration gave the DOT lead responsibility for pipeline security as well. In 2001, however, President Bush placed pipeline security authority within the newly-established Transportation Security Administration. Since its inception, TSA has administered a multifaceted pipeline security program centered around its corporate security reviews. The agency also inspects critical facilities, participates in security committees, and provides training, among many other activities.

While TSA has been engaged in a broad range of activities to help secure pipelines, questions remain about the overall structure and effectiveness of its pipeline security program. Three specific issues may warrant Congressional attention. No. 1, TSA's pipeline security resources. No. 2, voluntary versus mandatory standards. No. 3, uncertainty about pipeline security risks.

TSA's budget funds on the order of 10 to 15 full-time equivalent staff to support the various aspects of its pipeline security program. There is concern by some that this level of resources may not support rigorous and timely review of security plans and inspection of facilities Nation-wide. TSA's handful of pipeline staff accomplish a great deal, but they stand in contrast to over 700 staff in the other surface transportation modes at TSA, which excludes aviation. Over 500 pipeline safety staff available to the DOT. Given this disparity, it is logical to consider whether TSA's pipeline security resources should be increased, or whether DOT staff who inspect the same pipeline systems as TSA could somehow be deployed to help meet security objectives.

Although TSA has the statutory authority to regulate pipeline security, the agency has not promulgated such regulations. TSA asserts that its voluntary approach is more effective than mandatory standards. Canadian regulators, however, have come to a different conclusion. They do regulate pipeline security. Likewise, the U.S. Federal Energy Regulatory Commission has ordered mandatory cyber and physical security standards for the bulk electric power system which faces threats and vulnerabilities similar to pipelines. Canada's and FERC's decisions to regulate security raise questions as to the relative merits of a voluntary versus a regulatory approach to pipeline security.

TSA's pipeline threat assessment published in 2011 concluded with high confidence that the terrorist threat to the U.S. pipeline industry was low. No subsequent assessments are publicly available. However, recent events have increased concerns about pipeline system threats, especially cyber threats because the pipeline industry security risk assessments rely upon information from the Federal Government, uncertain or outdated threat information may lead to inconsistent security plans, inefficient spending of security resources, or deployment of security measures against the wrong threat.

In conclusion, the Nation's pipelines have proven to be both vulnerable to attacks and attractive to malicious actors. A strong Federal pipeline security program is clearly necessary. Real bombs have been planted, computer systems have been attacked, and perpetrators have been imprisoned. TSA identifies many activities under its Pipeline Security Program. But they are performed with constrained resources. While both the TSA and industry are engaged in pipeline security, questions have been raised as to their level of capability and how effective their efforts have actually been. Under TSA's current approach, it is difficult to know for certain.

Furthermore, while there have been no publicly-reported successful attacks on U.S. pipelines in recent years, existing security measures did not prevent attackers from planting explosive devices along U.S. pipelines on 2 separate occasions. If Congress concludes that TSA's current efforts are insufficient, it may decide to provide additional resources to support them, or specifically, direct TSA to develop pipeline security regulations. Congress also may direct TSA to focus additional attention on understanding pipeline threats, and to assess how the various elements of U.S. pipeline safety and security fit together.

Thank you for the opportunity to appear before the committee. I will be happy to answer any questions.

[The prepared statement of Mr. Parfomak follows:]

## PREPARED STATEMENT OF PAUL W. PARFOMAK

APRIL 19, 2016

Good morning Chairman Katko, Ranking Member Rice, and Members of the subcommittee. My name is Paul Parfomak, Specialist in Energy and Infrastructure Policy at the Congressional Research Service (CRS). CRS appreciates the opportunity to testify here today about the evolution of and current Federal role in pipeline security. Please note that, in accordance with our enabling statutes, CRS does not advocate policy or take a position on any related legislation.

### INTRODUCTION

Nearly 3 million miles of pipeline transporting natural gas, oil, and other hazardous liquids crisscross the United States. While an efficient and comparatively safe means of transport, these pipelines carry materials with the potential to cause public injury, destruction of property, and environmental damage. The Nation's pipeline network is also widespread, running alternately through remote and densely-populated regions. Pipelines are operated by increasingly sophisticated computer systems which manage their product flows and provide continuous information on their status. Due to their scale, physical exposure, and reliance on computer controls, pipelines are vulnerable to accidents, operating errors, and malicious attacks.

Congress has had long-standing concern about the security of the Nation's pipeline network. Beginning with the Aviation and Transportation Security Act of 2001 (Pub. L. 107–71), which established the Transportation Security Administration, and continuing through the PIPES Act of 2006 (Pub. L. 109–468) and the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. 110–53), Congress has enacted specific statutory provisions to help secure pipelines. Likewise, successive Presidential administrations have promulgated executive orders establishing a Federal framework for the security of pipelines, among other critical infrastructure. The 114th Congress is overseeing the implementation of the Federal pipeline security program and considering new legislation related to the Nation's pipeline systems. In particular, the SAFE PIPES Act (S. 2776), which reauthorizes the Federal pipeline safety program, would also mandate a report to Congress on the staffing, resource allocation, oversight strategy, and management of the Federal pipeline security program (§ 20).

### *Physical Threats to Pipeline Security*

Pipelines are vulnerable to intentional attacks using firearms, explosives, or other physical means. Oil and gas pipelines, globally, have been a favored target of terrorists, militant groups, and organized crime. For example, in 1996, London police foiled a plot by the Irish Republican Army to bomb gas pipelines and other utilities across the city.[1] In Colombia, rebels have bombed the Canon Lemon oil pipeline and other pipelines hundreds of times since 1993, most recently last March.[2] Likewise, militants in Nigeria have repeatedly attacked oil pipelines, including coordinated bombings of 3 pipelines in 2007 and the sophisticated bombing of an underwater pipeline in 2016.[3] A rebel group detonated bombs along Mexican oil and natural gas pipelines in July and September 2007.[4] Natural gas pipelines in British Columbia, Canada, were bombed 6 times between October 2008 and July 2009 by unknown perpetrators in acts classified by authorities as environmentally motivated "domestic terrorism."[5] In 2009, the *Washington Post* reported that over $1 billion of crude oil had been stolen directly from Mexican pipelines by organized criminals and drug cartels.[6]

Pipelines in the United States have also been targeted by terrorists and other malicious individuals. In 1999, Vancouver police arrested a man planning to bomb the Trans Alaska Pipeline System (TAPS) for personal profit in oil futures.[7] In 2005 a U.S. citizen sought to conspire with al-Qaeda to attack TAPS and a major natural gas pipeline in the eastern United States.[8] In 2006 Federal authorities acknowledged the discovery of a detailed posting on a website purportedly linked to al-Qaeda that reportedly encouraged attacks on U.S. pipelines, especially TAPS, using weapons or hidden explosives.[9] 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.[10] In 2011, a man planted a bomb,

---

[1] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, Washington, DC, October 1997.

[2] Luis Jaime Acosta, "Colombia's Canõ Limón Pipeline Suspended After Rebel Attacks," *Reuters,* March 14, 2016; Government Accountability Office (GAO), *Security Assistance: Efforts to Secure Colombia's Canõ Limón-Covenas Oil Pipeline Have Reduced Attacks, but Challenges Remain*, GAO–05–971, September 2005.

[3] Maggie Fick and Anjil Raval, "Bombed Pipeline to Hit Nigeria Oil Output," *Financial Times*, March 8, 2016; Katherine Houreld, "Militants Say 3 Nigeria Pipelines Bombed," *Associated Press,* May 8, 2007.

[4] Reed Johnson, "Six Pipelines Blown Up in Mexico," *Los Angeles Times*, September 11, 2007. p. A–3.

[5] Ben Gelinas, "New Letter Threatens Resumption of 'Action' against B.C. Pipelines," *Calgary Herald*, April 15, 2010.

[6] Steve Fainaru and William Booth, "Mexico's Drug Cartels Siphon Liquid Gold," *Washington Post,* December 13, 2009.

[7] David S. Cloud, "A Former Green Beret's Plot to Make Millions Through Terrorism," *Ottawa Citizen*, December 24, 1999, p. E15.

[8] U.S. Attorney's Office, Middle District of Pennsylvania, "Man Convicted of Attempting to Provide Material Support to Al-Qaeda Sentenced to 30 Years' Imprisonment," Press release, November 6, 2007; A. Lubrano and J. Shiffman, "Pa. Man Accused of Terrorist Plot," *Philadelphia Inquirer*, February 12, 2006, p. A1.

[9] Wesley Loy, "Web Post Urges Jihadists to Attack Alaska Pipeline," *Anchorage Daily News*, January 19, 2006.

[10] U.S. Department of Justice, "Four Individuals Charged in Plot to Bomb John F. Kennedy International Airport," press release, June 2, 2007.

which did not detonate, along a natural gas pipeline in Oklahoma.[11] In 2012, a man who reportedly had been corresponding with "Unabomber" Ted Kaczynski unsuccessfully bombed a natural gas pipeline in Plano, Texas.[12] To date, there have been no successful bombings of U.S. pipelines, but the threat of physical attacks remains credible.

### *Cyber Threats to Pipelines*

Although physical attacks on pipelines have been a focus in North America and elsewhere, the sophisticated computer systems used to operate pipeline systems are also vulnerable to cyber attacks. Cyber infiltration of supervisory control and data acquisition (SCADA) systems could allow "hackers" to disrupt pipeline service and cause spills, explosions, or fires—all from remote locations via the internet or other communication pathways. Such an approach reportedly was used to cause the 2008 explosion of the Baku-Tbilisi-Ceyhan oil pipeline in Turkey.[13]

In March 2012, the Industrial Control Systems Cyber Emergency Response Team housed within the Department of Homeland Security identified an on-going series of cyber intrusions among U.S. natural gas pipeline operators dating back to December 2011. According to the agency, various pipeline companies described targeted spear-phishing[14] attempts and intrusions into multiple natural gas pipeline sector organizations "positively identified . . . as related to a single campaign."[15] In 2011, computer security company McAfee reported similar "coordinated covert and targeted" cyber attacks originating primarily in China against global energy companies. The attacks began in 2009 and involved spear-phishing, exploitation of Microsoft software vulnerabilities, and the use of remote administration tools to collect sensitive competitive information about oil and gas fields.[16] In 2010, the Stuxnet computer worm was first identified as a threat to industrial control systems. Although the Stuxnet software initially spreads indiscriminately, the software includes a highly specialized industrial process component targeting specific industrial SCADA systems built by the Siemens company.[17] 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.

### *Potential Consequences of Pipeline Releases*

Although there have been no intentional releases from U.S. pipelines due to bombing or cyber attacks, accidental releases may illustrate the potential consequences of a successful attack. Pipeline accidents in the United States, on the whole, cause few fatalities compared to other product transportation modes, but such accidents have been catastrophic in several cases. For example, a 1999 gasoline pipeline accident in Bellingham, WA, killed 3 people and caused $45 million in damage to a city water plant and other property.[18] In 2000, a natural gas pipeline accident near Carlsbad, NM, killed 12 campers.[19] A 2010 natural gas pipeline explosion in San Bruno, CA, killed 8 people, injured 60 others, and destroyed 37 homes.[20] A

---

[11] U.S. Attorney's Office, "Konawa Man Sentenced for Attempting to Destroy or Damage Property Using an Explosive," press release, December 5, 2012.

[12] Valerie Wigglesworth, "Plano Blast Suspect Corresponded with Unabomber," *Dallas Morning News*, June 29, 2014; U.S. Attorney's Office, "Plano Man Guilty in Pipeline Bombing Incident," press release, June 3, 2013.

[13] Jordan Robertson and Michael Riley, "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar," *Bloomberg*, December 10, 2014.

[14] "Spear-phishing" involves sending official-looking e-mails to specific individuals to insert harmful software programs (malware) into protected computer systems; to gain unauthorized access to proprietary business information; or to access confidential data such as passwords, social security numbers, and private account numbers.

[15] Industrial Control Systems Cyber Emergency Response Team (ICS–CERT), "Gas Pipeline Cyber Intrusion Campaign," *ICS–CERT Monthly Monitor*, April 2012, p.1, *http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Apr2012.pdf*.

[16] McAfee Foundstone Professional Services and McAfee Labs, *Global Energy Cyberattacks: "Night Dragon,"* white paper, February 10, 2011, p. 3, *http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf*.

[17] Tobias Walk, "Cyber-attack Protection for Pipeline SCADA Systems," *Pipelines International Digest*, January 2012, p. 7.

[18] National Transportation Safety Board, *Pipeline Rupture and Subsequent Fire in Bellingham, Washington June 10, 1999*, NTSB/PAR–02/02, October 8, 2002.

[19] National Transportation Safety Board, *Natural Gas Pipeline Rupture and Fire Near Carlsbad, New Mexico August 19, 2000*, NTSB/PAR–03–01, February 11, 2003.

[20] National Transportation Safety Board, *Pacific Gas and Electric Company Natural Gas Transmission Pipeline Rupture and Fire, San Bruno, California, September 9, 2010*, NTSB/PAR–11/01, August 30, 2011.

2010 pipeline spill released 819,000 gallons of crude oil into a tributary of the Kalamazoo River near Marshall, MI.[21] A 2014 natural gas distribution pipeline explosion in New York City killed 8 people, injured 50 others, destroyed 2 5-story buildings, and caused the temporary closure of a transit line due to debris.[22] Such accidents demonstrate the potential risk to human life, property, and the environment. Disruption of service from these pipelines also caused economic and operational impacts among the pipelines' customers. Such accidents have generated substantial scrutiny of pipeline regulation and increased State and community activity related to pipeline safety and security.[23]

### THE FEDERAL ROLE IN PIPELINE SECURITY

Federal pipeline security efforts originated in the pipeline safety program. The Natural Gas Pipeline Safety Act of 1968 (Pub. L. 90–481) and the Hazardous Liquid Pipeline Act of 1979 (Pub. L. 96–129) are 2 of the principal early acts establishing the Federal role in pipeline safety. Under both statutes, the Transportation Secretary is given primary authority to regulate key aspects of inter-State pipeline safety: Design, construction, operation and maintenance, and spill response planning. At the end of fiscal year 2015, the Department of Transportation (DOT) employed 234 pipeline safety staff in its Pipeline and Hazardous Materials Safety Administration (PHMSA).[24] In addition to its own staff, PHMSA's enabling legislation allows the agency to delegate authority to intra-State pipeline safety offices, and allows State offices to act as "agents" administering inter-State pipeline safety programs (excluding enforcement) for those sections of inter-State pipelines within their boundaries.[25] There were approximately 330 full-time equivalent State pipeline safety inspectors in 2015.[26]

Presidential Decision Directive 63, issued by the Clinton administration in 1998, assigned to the DOT lead responsibility for pipeline security as well as safety.[27] Under this authority, after the terrorist attacks of September 11, 2001, the DOT conducted a vulnerability assessment to identify critical pipeline facilities and worked with industry groups and State pipeline safety organizations to assess the industry's readiness to prepare for, withstand, and respond to a terrorist attack.[28] Together with the Department of Energy and State pipeline agencies, the DOT promoted the development of consensus standards for security measures[29] tiered to correspond with the 5 levels of threat warnings issued by the Office of Homeland Security.[30] The DOT also developed protocols for inspections of critical facilities to ensure that operators implemented appropriate security practices. To convey emergency information and warnings, the DOT established a variety of communication links to key staff at the most critical pipeline facilities throughout the country. The DOT also began identifying near-term technology to enhance deterrence, detection, response, and recovery, and began seeking to advance public and private-sector planning for response and recovery.[31]

---

[21] National Transportation Safety Board, *Enbridge, Inc. Hazardous Liquid Pipeline Rupture*, Board meeting summary, July 25, 2010, *http://www.ntsb.gov/news/events/2012/marshall_mi/index.html*.

[22] National Transportation Safety Board, *Natural Gas-Fueled Building Explosion and Resulting Fire New York City, New York March 12, 2014*, NTSB/PAR–15/01, June 9, 2015.

[23] See, for example: Jim Lynch and Jonathan Oosting, "Opposition Grows to Straits of Mackinac Oil Lines," *Detroit News*, April 13, 2016; Bellingham Herald Editorial Board, "Citizens Need Panel To Monitor Pipeline Safety," Bellingham Herald (WA), January 24, 2010; Janet Zink, "Fueling the Resistance," *St. Petersburg Times*, December 16, 2007; J. Nesmith and R.K.M. Haurwitz, "Pipelines: The Invisible Danger," *Austin American-Statesman*, July 22, 2001.

[24] Artealia Gilliard, PHMSA, personal communication, September 18, 2015. Employees as of September 18, 2015.

[25] 49 U.S.C. 60107.

[26] Artealia Gilliard, September 9, 2015.

[27] Presidential Decision Directive 63, *Protecting the Nation's Critical Infrastructures*, May 22, 1998.

[28] Research and Special Programs Administration (RSPA), *RSPA Pipeline Security Preparedness*, December 2001.

[29] See: American Petroleum Institute and National Petrochemical and Refiners Association, *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries*, March 2002; Interstate Natural Gas Association of America (INGAA) and American Gas Association (AGA), *Security Guidelines for the Natural Gas Industry*, September 2002.

[30] Ellen Engleman, Administrator, Research and Special Programs Administration (RSPA), statement before the Subcommittee on Energy and Air Quality, House Energy and Commerce Committee, March 19, 2002.

[31] Ellen Engleman, Administrator, Research and Special Programs Administration (RSPA), statement before the Subcommittee on Highways and Transit, House Transportation and Infrastructure Committee, February 13, 2002.

In September 2002, the DOT circulated formal guidance developed in cooperation with the pipeline industry associations defining the agency's security program recommendations and implementation expectations. This guidance recommended that operators identify critical facilities, develop security plans consistent with prior trade association security guidance, implement these plans, and review them annually.[32] While the guidance was voluntary, the DOT expected compliance and informed operators of its intent to begin reviewing security programs within 12 months, potentially as part of more comprehensive safety inspections.[33]

### *Transferring Pipeline Security to TSA*

In November 2001, President Bush signed the Aviation and Transportation Security Act (Pub. L. 107–71) establishing the Transportation Security Administration (TSA) within the DOT. According to TSA, the act placed the DOT's pipeline security authority (under PDD–63) within TSA. The act specified for TSA a range of duties and powers related to general transportation security, such as intelligence management, threat assessment, mitigation, and security measure oversight and enforcement, among others. On November 25, 2002, President Bush signed the Homeland Security Act of 2002 (Pub. L. 107–296) creating the Department of Homeland Security (DHS). Among other provisions, the act transferred to DHS the Transportation Security Administration from the DOT (§ 403). On December 17, 2003, President Bush issued Homeland Security Presidential Directive 7 (HSPD–7), clarifying executive agency responsibilities for identifying, prioritizing, and protecting critical infrastructure.[34] HSPD–7 maintains DHS as the lead agency for pipeline security (par. 15), and instructs the DOT to "collaborate in regulating the transportation of hazardous materials by all modes (including pipelines)" (par. 22h). The order requires that DHS and other Federal agencies collaborate with "appropriate private sector entities" in sharing information and protecting critical infrastructure (par. 25). TSA joined both the Energy Government Coordinating Council and the Transportation Government Coordinating Council under provisions in HSPD–7. The missions of the councils are to work with their industry counterparts to coordinate critical infrastructure protection programs in the energy and transportation sectors, respectively, and to facilitate the sharing of security information.

HSPD–7 also required DHS to develop a National plan for critical infrastructure and key resources protection (par. 27), which the agency issued in 2006 as the National Infrastructure Protection Plan (NIPP). The NIPP, in turn, required each critical infrastructure sector to develop a Sector-Specific Plan (SSP) that describes strategies to protect its critical infrastructure, outlines a coordinated approach to strengthen its security efforts, and determines appropriate funding for these activities. Executive Order 13416 further required the transportation sector SSP to prepare annexes for each mode of surface transportation.[35] In accordance with the above requirements the TSA issued its *Transportation Systems Sector-Specific Plan and Pipeline Modal Annex* in 2007 with an update on 2010.

## TSA'S PIPELINE SECURITY ACTIVITIES

Although the TSA has regulatory authority for pipeline security under Pub. L. 107–71 and Pub. L. 110–53, its activities to date have relied upon voluntary industry compliance with the agency's security guidance and best practice recommendations.[36] TSA has administered a multifaceted program to facilitate these efforts. In 2003, TSA initiated its on-going Corporate Security Review (CSR) program, wherein the agency visits the largest pipeline and natural gas distribution operators to review their security plans and inspect their facilities. During the reviews, TSA evaluates whether each company is following the intent of the DOT's voluntary security guidance, as updated by TSA, and seeks to maintain the list of assets each company has identified meeting the criteria established for critical facilities. In 2008, the TSA initiated its Critical Facility Inspection Program (CFI), under which the agency conducted in-depth inspections of all the critical facilities of the 125 largest pipeline systems in the United States. The agency estimated that these 125 pipeline systems

---

[32] James K. O'Steen, Research and Special Programs Administration (RSPA), *Implementation of RSPA Security Guidance*, presentation to the National Association of Regulatory Utility Commissioners, February 25, 2003.

[33] James K. O'Steen, Office of Pipeline Safety (OPS), personal communication, June 10, 2003.

[34] HSPD–7 supersedes PDD–63 (par. 37).

[35] Executive Order 13416, "Strengthening Surface Transportation Security," December 5, 2006.

[36] Transportation Security Administration, *Pipeline Security Guidelines*, April 2011, and *Pipeline Security Smart Practice Observations*, September 19, 2011.

collectively included approximately 600 distinct critical facilities.[37] TSA concluded the initial round of CFI inspections in 2011, having completed a total of 347 site visits throughout the United States.[38]

Over the last decade, TSA has engaged in a number of additional pipeline security initiatives, including:

- Developing a statistical tool used for relative risk ranking and prioritization,
- Completing a security incident and recovery protocol plan mandated under Pub. L. 110–53,
- Initiating a program to address risks from pipeline transportation of hazardous materials other than oil and natural gas,
- Assessing U.S. and Canadian security and planning for critical cross-border pipelines,
- Convening international pipeline security forums for U.S. and Canadian governments and pipeline industry officials,
- Facilitating pipeline security drills and exercises including those under the Intermodal Security Training Exercise Program (I–STEP),
- Developing pipeline security awareness training materials,
- Convening periodic information-sharing conference calls between key pipeline security stakeholders, and
- Participating in Sector Coordinating Councils and Joint Sector Committees.[39]

In addition to these activities, TSA has also conducted regional supply studies for key natural gas markets, has conducted training on cybersecurity awareness, has participated in pipeline blast mitigation studies, and has joined in "G–8" multinational security assessment and planning.[40]

*Pipeline Cybersecurity Initiatives*

Pipeline cybersecurity is an element of several Federal initiatives within DHS.[41] For example, TSA has included a number of general cybersecurity provisions in its industry security guidance[42] and has encouraged industry compliance with the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*.[43] TSA has also employed the *http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.*

Cybersecurity Assessment and Risk Management Approach (CARMA) in collaborating with key stakeholders to identify pipeline industry value chains, critical functions, and supporting cyber infrastructure.[44] The agency has also coordinated with DHS and the Department of Energy to harmonize existing cybersecurity risk management programs. Pipelines are also included in DHS's multi-modal cybersecurity initiatives, such as its Industrial Control Systems Cyber Emergency Response Team (ICS–CERT).[45] The TSA also has established a public/private partnership-based cybersecurity program supporting the National Infrastructure Protection Plan. Pipeline operators have participated in DHS-sponsored control systems cybersecurity

---

[37] Department of Homeland Security, "Extension of Agency Information Collection Activity Under OMB Review: Critical Facility Information of the Top 100 Most Critical Pipelines," 76 *Federal Register* 62818, October 11, 2011.

[38] Jack Fox, General Manager, Pipeline Security Division, Transportation Security Administration, personal communication, February 24, 2012.

[39] Jack Fox, Pipeline Industry Engagement Manager, TSA, *Pipeline Security: An Overview of TSA Programs*, slide presentation, May 5, 2014; Transportation Security Administration, *Transportation Systems Sector-Specific Plan, 2010*, p. 326.

[40] Transportation Security Administration, Pipeline Modal Annex, June 2007, pp. 10–11. G8=Group of Eight (the United States, the United Kingdom, Canada, France, Germany, Italy, Japan, and Russia).

[41] The Interstate Natural Gas Association of America (INGAA), a trade association for gas pipeline companies, maintains its own extensive cybersecurity guidelines for natural gas pipeline control systems: INGAA, *Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry*, Washington, DC, January 31, 2011. Likewise, the American Petroleum Institute (API), a trade association within the oil industry, maintains a standard for oil pipeline control system security: API, *Pipeline SCADA Security*, Second Edition, API Std. 1164, Washington, DC, June 2009.

[42] For example, TSA's guidance advises operators to "conduct a risk assessment to weigh the benefits of implementing wireless networking against the potential risks for exploitation." TSA, April 2011, p. 18.

[43] Jack Fox, Pipeline Industry Engagement Manager, TSA, personal communication, October 29, 2015. See: National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2014, *http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf*.

[44] Jack Fox, May 5, 2014.

[45] Department of Homeland Security, "Industrial Control Systems Cyber Emergency Response Team (ICS–CERT)," web page, April 13, 2106, *https://ics-cert.us-cert.gov/*.

training and also participate in the DHS Industrial Control Systems Joint Working Group.[46]

Outside DHS, the Department of Energy operates the National SCADA Test Bed Program, a partnership with Idaho National Laboratory, Sandia National Laboratories, and other National laboratories which addresses control system security challenges in the energy sector. Among its key functions, the program performs control systems testing, research and development; control systems requirements development; and industry outreach.[47] Sandia Laboratories also performs authorized defensive cybersecurity assessments for Government, military, and commercial customers through its Information Design Assurance Red Team (IDART) program.[48]

*The Relationship Between DOT and TSA*

Since TSA was established, Congress has had a continuing interest in the appropriate division of pipeline security authority between the DOT and TSA.[49] Both the DOT and TSA have played important roles in the Federal pipeline security program, with TSA the designated lead agency since 2002. In 2004, the DOT and DHS entered into a memorandum of understanding (MOU) concerning their respective security roles in all modes of transportation. The MOU notes that DHS has the primary responsibility for transportation security with support from the DOT, and establishes a general framework for cooperation and coordination. On August 9, 2006, the departments signed an annex "to delineate clear lines of authority and responsibility and promote communications, efficiency, and nonduplication of effort through cooperation and collaboration between the parties in the area of transportation security."[50]

In January 2007, DOT officials testified before Congress that the agency had established a joint working group with TSA "to improve interagency coordination on transportation security and safety matters, and to develop and advance plans for improving transportation security," presumably including pipeline security.[51] According to TSA, the working group developed a multi-year action plan specifically delineating roles, responsibilities, resources, and actions to execute 11 program elements: Identification of critical infrastructure/key resources and risk assessments; strategic planning; developing regulations and guidelines; conducting inspections and enforcement; providing technical support; sharing information during emergencies; communications; stakeholder relations; research and development; legislative matters; and budgeting.[52] Nonetheless, a DOT Inspector General (IG) assessment published May 2008 was not satisfied with this plan. The IG report stated that, although the agencies

> "have taken initial steps toward formulating an action plan to implement the provisions of the pipeline security annex . . . further actions need to be taken with a sense of urgency because the current situation is far from an 'end state' for enhancing the security of the Nation's pipelines."[53]

The assessment recommended that the DOT and TSA finalize and execute their security annex action plan, clarify their respective roles, and jointly develop a pipeline security strategy that maximizes the effectiveness of their respective capabilities

---

[46] Department of Homeland Security, "Industrial Control Systems Joint Working Group (ICSJWG)," web page, April 13, 2016, *https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG*.

[47] U.S. Department of Energy, "National SCADA Test Bed," web page, August 13, 2016, *http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed*.

[48] Sandia National Laboratories, "The Information Design Assurance Red Team (IDART)," web page, August 13, 2016, *http://www.idart.sandia.gov/*.

[49] For example, see Hon. William J. Pascrell, Jr., statement at the House Committee on Transportation and Infrastructure, Subcommittee on Highways, Transit, and Pipelines, hearing on Pipeline Safety, March 16, 2006.

[50] Transportation Security Administration and Pipelines and Hazardous Materials Safety Administration, "Transportation Security Administration and Pipelines and Hazardous Materials Safety Administration Cooperation on Pipelines and Hazardous Materials Transportation Security," August 9, 2006.

[51] Barrett, T.J., Administrator, Pipeline and Hazardous Materials Safety Administration (PHMSA), Testimony before the Senate Committee on Commerce, Science, and Transportation hearing on Federal Efforts for Rail and Surface Transportation Security, January 18, 2007.

[52] Transportation Security Administration, Pipeline Security Division, personal communication, July 6, 2007.

[53] U.S. Dept. of Transportation, Office of Inspector General, *Actions Needed to Enhance Pipeline Security, Pipeline and Hazardous Materials Safety Administration*, Report No. AV–2008–053, May 21, 2008, p. 3.

and efforts.[54] According to TSA, working with the DOT "improved drastically" after the release of the IG report; the 2 agencies began maintaining daily contact, sharing information in a timely manner, and collaborating on security guidelines and incident response planning.[55]

## KEY POLICY ISSUES

While the Federal Government has been engaged in various efforts to protect the Nation's oil and natural gas pipelines from deliberate attacks since September 11, 2001, questions remain regarding the structure and effectiveness of these efforts. Three specific issues, in particular, may warrant further Congressional consideration: (1) TSA's pipeline security resources, (2) voluntary versus mandatory security standards, and (3) uncertainty about security risks to the Nation's pipeline network.

### *TSA Pipeline Security Resources*

Some Members of Congress have been critical in the past of TSA's level of funding of non-aviation security activities, including pipeline activities. For example, as one Member remarked in 2005, "aviation security has received 90% of TSA's funds and virtually all of its attention. There is simply not enough being done to address . . . pipeline security."[56] At a Congressional hearing in 2010, another Member expressed concern that TSA's pipeline division did not have sufficient staff to carry out a Federal pipeline security program on a National scale.[57] With respect to pipeline security funding, little may have changed since 2005. The President's fiscal year 2017 budget request for DHS does not include a separate line item for TSA's pipeline security activities. The budget does request $110.8 million for "Surface Transportation Security," which encompasses security activities in non-aviation transportation modes, including pipelines. The budget would fund 761 full-time equivalent (FTE) employees.[58] TSA's pipeline branch has traditionally received from the agency's general operational budget an allocation for routine operations, travel, and outreach. The budget historically has funded on the order of 10 to 15 FTE staff to carry out the agency's pipeline security program.[59]

At its current staffing level, TSA's pipelines branch has limited field presence for pipeline site visits, and has constrained capabilities for updating standards, interacting in the various stakeholder groups with which it collaborates, analyzing security information, and fulfilling other administrative responsibilities. In conducting a pipeline corporate security review, for example, TSA typically sends 1 to 3 staff to hold a 3- to 4-hour interview with the operator's security representatives followed by a visit to only 1 or 2 of the operator's pipeline assets.[60] There is concern by some that the agency's CSRs (as currently structured) may not allow for rigorous security plan verification nor a credible threat of enforcement, so operator compliance with security guidance is uncertain. The limited number of CSR's the agency can complete in a year has also been a concern to some, even within TSA. According to a 2009 Government Accountability Office report, "TSA's pipeline division stated that they would like more staff in order to conduct its corporate security reviews more frequently," in part because other staff responsibilities such as "analyzing secondary or indirect consequences of a terrorist attack and developing strategic risk objectives required much time and effort."[61]

TSA's handful of field inspection staff stands in contrast to the hundreds of pipeline safety inspection staff available to the DOT at the Federal and State levels. Furthermore, in the face of an expanding U.S. pipeline network and evolving safety requirements, DOT's budget authority for pipeline safety has more than doubled

---

[54] Ibid. pp. 5–6.

[55] Jack Fox, TSA, Pipeline Security Division, personal communication, February 2, 2010.

[56] Sen. Daniel K. Inouye, opening statement before the Senate Committee on Commerce, Science, and Transportation, hearing on the President's Fiscal Year 2006 Budget Request for the Transportation Security Administration (TSA), February 15, 2005.

[57] Congressman Gus M. Billirakis, Remarks before the House Committee on Homeland Security, Subcommittee on Management, Investigations, and Oversight hearing on "Unclogging Pipeline Security: Are the Lines of Responsibility Clear?", Plant City, FL, April 19, 2010.

[58] U.S. Office of Management and Budget, *Budget of the United States Government, Fiscal Year 2017: Appendix*, February 2016, p. 537.

[59] Jack Fox, October 29, 2015.

[60] Department of Homeland Security, "Intent to Request Approval from OMB of One New Public Collection of Information: Pipeline Corporate Security Review," 74 *Federal Register* 42086, August 20, 2009.

[61] U.S. Government Accountability Office, *Transportation Security: Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation*, GAO–09–492, March 2009, p. 30, *http://www.gao.gov/new.items/d09492.pdf*.

over the last 10 years.[62] Given this disparity, it may be logical to consider whether DOT's field staff, who are charged with inspecting the same pipeline systems as TSA, could somehow be deployed to help fulfill the Nation's pipeline security objectives. The question also arises whether having separate inspections of the same pipeline systems for safety and security may be inherently inefficient, or may miss an opportunity for more frequent or thorough examination of pipeline security. Presumably many of the jurisdictional, operational, or administrative issues that were considered in the drafting of the 2004 MOU between DOT and TSA remain unchanged, but new factors—such as the evolving threat environment or greater experience with pipeline company security efforts—could warrant a reconsideration of the relationship between the agencies.

### *Voluntary vs. Mandatory Pipeline Security Standards*

Federal pipeline security activities to date have relied upon voluntary industry compliance with DOT's original security guidance, which later became TSA's security best practices. By initiating this voluntary approach in 2002, DOT sought to speed adoption of security measures by industry and avoid the publication of sensitive security information (e.g., critical asset lists) that would normally be required in public rulemaking.[63] However, a key subject of debate is the adequacy of the TSA's voluntary approach to pipeline security, generally, and cybersecurity, in particular. For example, provisions in the Pipeline Inspection, Protection, Enforcement, and Safety Act of 2006 (Pub. L. 109–468) required the DOT Inspector General (IG) to "address the adequacy of security standards for gas and oil pipelines" (§ 23(b)(4)). The 2008 IG's report stated that:

> "TSA's current security guidance is not mandatory and remains unenforceable unless a regulation is issued to require industry compliance . . . [DOT] and TSA will need to conduct covert tests of pipeline systems' vulnerabilities to assess the current guidance as well as the operators' compliance."[64]

Although the IG report did not elaborate on this recommendation, covert testing of vulnerabilities would likely include testing of both physical security measures and cybersecurity measures. The latter would be in place to protect pipeline SCADA systems and sensitive operating information such as digital pipeline maps, system design data, and emergency response plans. Consistent with the IG's recommendation, an April 2011 White House proposal[65] and the Cybersecurity Act of 2012 (S. 2105) both would have mandated the promulgation of cybersecurity regulations for pipelines, among other provisions, although these proposals would not necessarily have conferred upon TSA any authority it does not already have to regulate pipeline security.

In contrast to the IG's conclusions and the legislative proposals above, the pipeline industry has consistently expressed concern that security regulations could be "redundant" and "may not be necessary to increase pipeline security."[66] Echoing this sentiment, a DOT official testified in 2007 that enhancing security "does not necessarily mean that we must impose regulatory requirements."[67]

TSA officials have similarly questioned the need for new pipeline security regulations, particularly the IG's call for covert testing of pipeline operator security measures. The TSA has argued in the past that the agency is complying with the letter of Pub. L. 110–53 and that its pipeline operator security reviews are more than paper reviews.[68] TSA officials assert that security regulations could be counter-

---

[62] U.S. Office of Management and Budget, *Budget of the United States Government, Appendix*, Fiscal Years 2006 through 2017, "Pipeline Safety," Line 1900 "Budget authority (total)."

[63] GAO, *Pipeline Security and Safety: Improved Workforce Planning and Communication Needed*, GAO–02–785, August 2002, p. 22.

[64] U.S. Dept. of Transportation, Office of Inspector General, May 21, 2008, p. 6.

[65] The White House, "Legislative Language, Cybersecurity Regulatory Framework for Covered Critical Infrastructure," April 2011, p. 33, *http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security-full-bill.pdf*.

[66] American Gas Association (AGA), American Petroleum Institute (API), Association of Oil Pipe Lines (AOPL), and American Public Gas Association (APGA), joint letter to Members of the Senate Commerce Committee providing views on S. 1052, August 22, 2005.

[67] T.J. Barrett, Administrator, Pipeline and Hazardous Materials Safety Administration, Department of Transportation, Testimony before the Senate Committee on Commerce, Science, and Transportation hearing on Federal Efforts for Rail and Surface Transportation Security, January 18, 2007.

[68] John Sammon, Transportation Security Administration, Testimony before the House Transportation and Infrastructure Committee, Railroad, Pipelines, and Hazardous Materials Subcommittee hearing on Implementation of the Pipeline Inspection, Protection, Enforcement, and Safety Act of 2006, June 24, 2008.

productive because they could establish a general standard below the level of security already in place at many pipeline companies based on their company-specific security assessments. Because the TSA believes the most critical U.S. pipeline systems generally meet or exceed industry security guidance, the agency asserts that it achieves better security with voluntary guidelines, and maintains a more cooperative and collaborative relationship with its industry partners as well.[69]

The Energy Sector Control Systems Working Group makes related assertions in its *Roadmap to Achieve Energy Delivery Systems Cybersecurity* about the effectiveness of cybersecurity standards alone:

> "Although standards may elevate cybersecurity across the energy sector, they do so by requiring the implementation of minimum security measures that set a baseline for cybersecurity across an industry. These minimum security levels may not be sufficient to secure the sector against new and quickly evolving risks. Asset owners compliant with standards may still be vulnerable to cyber intrusion."[70]

Thus, in addition to cybersecurity requirements, pipeline companies may also need appropriate management practices, performance metrics, access to intelligence, and other support measures to maximize the effectiveness of their cybersecurity programs.

Although the TSA believes a voluntary approach to pipeline security is most effective, Canadian pipeline regulators have come to a different conclusion. In 2010 the National Energy Board (NEB) of Canada mandated security regulations for jurisdictional Canadian petroleum and natural gas pipelines, some of which are cross-border pipelines entering the United States. Many companies operate pipelines in both countries. In announcing these new regulations, the board stated that it had considered adopting the existing cybersecurity standards "as guidance" rather than an enforceable standard, but "taking into consideration the critical importance of energy infrastructure protection," the board decided to adopt the standard into the regulations.[71] Establishing pipeline security regulations in Canada is not completely analogous to doing so in the United States as the Canadian pipeline system is much smaller and operated by far fewer companies than the U.S. system. Nonetheless, Canada's choice to regulate pipeline security may raise questions as to why the United States has not.

The Federal Energy Regulatory Commission (FERC), which regulates the U.S. bulk electric power system, has also taken a more directive approach to infrastructure security. The Energy Policy Act of 2005 (Pub. L. 109–58) gave the commission authority to oversee the reliability of the bulk power system, including authority to approve mandatory security standards. FERC approved mandatory Critical Infrastructure Protection cybersecurity reliability standards in 2008.[72] The commission approved mandatory physical security standards in 2014[73] after a successful physical attack on a high-voltage transformer facility in California. While it differs in important ways from the pipeline system, the bulk power system faces the same threat environment and has many similar security vulnerabilities related to asset exposure and reliance on SCADA systems for network operations.

In addition to examining the regulatory motivations of the NEB and FERC, consideration of mandatory pipeline security standards within TSA would have to account for the requirements to implement such standards. Unlike maintaining voluntary standards, developing pipeline security regulations—with provisions for pipeline operations, inspection, reporting, and enforcement—would involve a complex and potentially contentious rulemaking process involving multiple stakeholders. Should Congress choose to mandate the promulgation of such regulations, it is not clear that TSA's pipeline security division as currently configured would be up to

---

[69] John Pistole, Administrator, TSA, testimony before the Senate Committee on Commerce, Science, and Transportation hearing on Transportation Security Administration Oversight: Confronting America's Transportation Security Challenges, April 30, 2014; Jack Fox, General Manager, Pipeline Security Division, TSA, Remarks before the Louisiana Gas Association Pipeline Safety Conference, New Orleans, LA, July 25, 2012.

[70] Energy Sector Control Systems Working Group, Roadmap to Achieve Energy Delivery Systems Cybersecurity, September 2011, p. 15.

[71] National Energy Board of Canada, *Proposed Regulatory Change (PRC) 2010–01, Adoption of CSA Z246.1–09 Security Management for Petroleum and Natural Gas Industry Systems*, File Ad–GA–SEC–SecGen 0901, May 3, 2010, p. 1, *https://www.neb-one.gc.ca/ll-eng/livelink.exe/fetch/2000/90463/409054/614444/A1S7H7__Proposed__Regulatory____*Change*__(PRC)__2010-01.pdf?nodeid=614556&vernum=0.*

[72] Federal Energy Regulatory Commission, *Mandatory Reliability Standards for Critical Infrastructure Protection*, Docket No. RM06–22–000, Order No. 706, January 18, 2008.

[73] Federal Energy Regulatory Commission, *Physical Security Reliability Standard*, Docket No. RM14–15–000, Order No. 802, Issued November 20, 2014.

the task. Developing specific cybersecurity regulations may pose a particular challenge as the TSA's pipeline branch has limited existing capability to do so, although such capabilities may reside elsewhere in DHS. If mandatory standards were to be imposed, there may also be questions as to whether the agency as currently structured would have sufficient resources to implement the new security regulations, conduct rigorous security plan verification, and pose a credible threat of enforcement.

### *Uncertainty About Security Risks*

A January 2011 Federal threat assessment concluded "with high confidence that the terrorist threat to the U.S. pipeline industry is low."[74] However, subsequent events may have increased concerns about pipeline system threats, especially cyber threats. In a 2016 *Federal Register* notice, TSA stated that it expects pipeline companies will report approximately 30 "security incidents" annually—both physical and cyber.[75] The agency has not publicly released a more current pipeline threat assessment.

The pipeline industry's security risk assessments rely upon information about security threats provided by the Federal Government and by pipeline operators themselves. The quantity, quality, and timeliness of this threat information is a key determinant of what pipeline companies need to be protecting against, and what security measures to take. Incomplete or ambiguous threat information—especially from the Federal Government—may lead to inconsistency in physical and cybersecurity among pipeline owners, inefficient spending of limited security resources at facilities (e.g., that may not really be under threat), or deployment of security measures against the wrong threat.

Concerns about the quality and specificity of Federal threat information have long been an issue across all critical infrastructure sectors.[76] Threat information continues to be an uncertainty in the case of pipeline network security. There may be agreement among Government and industry stakeholders that oil and natural gas pipelines in the United States are vulnerable to attack, and that such attacks potentially could have catastrophic consequences. But the most serious, damaging attacks could require operational information and a certain level of sophistication, especially in the cyber regime, on the part of potential attackers. Consequently, despite the technical arguments, without more specific information about potential targets and attacker capabilities, the true risk of a serious attack on the pipeline system remains an open question.

## CONCLUSION

The Nation's pipeline network is attractive to malicious actors and vulnerable to both physical and cyber attacks. Based on recent history, a strong Federal pipeline security program is clearly necessary; there has been a series of unrelated terrorist plots and attempted attacks on U.S. pipelines since at least the 1990s. Real bombs have been planted, computers systems have been infiltrated, and perpetrators have been imprisoned. Such threats to the pipeline system are likely to continue.

Both Government and industry have taken numerous steps to improve pipeline security since 2001. On their face, these measures have been expansive and seem to address the full range of activities and priorities Congress intended when it embarked upon a National strategy for protecting critical infrastructure. However, while TSA and industry may be engaged in appropriate pipeline security activities, questions remain as to their level of commitment to those activities and how effective they have been in protecting the pipeline system. TSA's pipeline staff would account for less than 2% of the agency's surface transportation security staff under the proposed fiscal year 2017 budget, and just over 2% of the staff available to DOT under its pipeline safety program. Pipeline company expenditures on security are not generally reported, so their level of financial commitment is unknown. Furthermore, while there have been no publicly reported successful attacks on the U.S. pipeline system since 2001, existing physical security measures did not prevent 2 attackers from planting the live explosive devices along 2 different U.S. pipelines in 2011 and 2012 discussed earlier. Their failure to detonate was fortunate.

The TSA maintains that its pipeline security program, administered as it is and relying upon voluntary standards, has been effective in protecting U.S. pipelines from physical and cyber attacks. Based on the agency's corporate security reviews,

---

[74] Transportation Security Administration, Office of Intelligence, *Pipeline Threat Assessment*, January 18, 2011, p. 3.

[75] 81 *Fed. Reg*. 37, February 25, 2016, p. 94–95.

[76] See, for example, Philip Shenon, "Threats and Responses: Domestic Security," *New York Times*, June 5, 2003, p. A15.

TSA believes security among major U.S. pipeline systems is good, and pipeline operators agree. However, without formal security plans and reporting requirements, it is difficult for Congress and the general public to know for certain. To a great extent, the public must therefore rely on the pipeline industry's self-interest to protect itself from malicious threats. Whether this self-interest is sufficient to generate the level of security appropriate for a critical infrastructure sector, and whether imposing mandatory standards would be a better approach, is open to debate. Faced with this uncertainty, legislators must rely upon their own best judgment to reach conclusions about the Federal pipeline security program. If Congress concludes that current voluntary measures are insufficient to protect the pipeline system, it may decide to provide specific direction to the TSA to develop regulations and provide additional resources to support them, as such an effort may be beyond the TSA pipeline branch's existing capabilities.

Congress also may assess how the various elements of U.S. pipeline safety and security activity fit together in the Nation's overall strategy to protect critical infrastructure. For example, diverting pipeline resources away from safety to enhance security might further reduce terror risk, but not overall pipeline risk, if safety programs become less effective as a result. Pipeline safety and security necessarily involve many groups: Federal and State agencies, oil and gas pipeline associations, large and small pipeline operators, and local communities. Reviewing how these groups work together to achieve common goals could be an oversight challenge for Congress.

Mr. KATKO. Thank you, Dr. Parfomak for your testimony. We appreciate you being here as well.

I now recognize myself for 5 minutes of questions.

I want to start by saying I understand the overall setup here. The Department of Transportation is in charge of and oversees the safety aspects of the pipelines, which includes making sure when a guy has a backhoe and, you know, digs where he shouldn't dig, that they respond properly and they have the right procedures in place to cut off that pipeline.

I also understand that on the other side you have security aspects which is TSA's oversight. At first glance it looks like kind-of an odd setup. But it, by all indications from the industry, it does seem to work. But there are things that I want to talk about. While I am happy that you are all happy, I just want to make sure that we are not missing something here. So I will be checking on some of the things I have concerns with.

The first thing is probably the easiest thing. That is for Mr. Black. That is with respect to PHMSA and the oil pipeline response plans. What would be your suggestion of a way to make sure that those things don't get disclosed to the public when they are submitted to Congress?

Mr. BLACK. PHMSA has done the right thing. PHMSA's chief counsel has issued guidance to PHMSA staff that the information in part 60138, of the last pipeline safety law, can be redacted. They have said that it should be. So what we are looking for is Congress, when enacting legislation to receive these response plans, to make sure you have clear and consistent procedures.

I am happy to follow up with a specific proposal. But a couple of principles. No. 1, there needs to be a clear statement that this information should remain confidential and should not be transmitted to anybody outside of Congressional staff in any form.

Second, there need to be some specific procedures applied to that. I am sure this committee has some specific procedures for certain types of information. Those need to be connected. For example, a secure reading room, tracking who goes in and who goes out of that reading room with information.

Then, third, we suggest a penalty or some type of a disciplinary mechanism for those people that violate it. We need to make sure that this information is secured and is not put into the wrong hands while you conduct that oversight that you need to do.

Mr. KATKO. Okay. Thank you very much.

Now, the other areas I am concerned about, and if I don't hit on them I hope my colleagues on the panel do, are whether the 2011 guidelines issued by TSA need to be upgraded, the sharing and use of actionable information and how sometimes when TSA gets secret information that may be helpful, how they are able to share that and how can we make that process better sharing it with the private sector. Then of course the things that CRS raised, the resources issue, the voluntary versus mandatory guidelines issue, and what is a level of risk. So let's just start at the top of the list here, and I will work through as much as I can.

The 2011 guidelines were promulgated prior to the dramatic rise of ISIS and the new and dynamic threat that they propose. So given that and all the other factors, I know that it doesn't seem to be a high level of threat in the United States where pipeline attacks, but they have shown a propensity to do those attacks elsewhere, including even Canada.

So given all that and given the rise of ISIS, do you think it is time for TSA to issue an updated guidelines?

Ms. PROCTOR. Mr. Chairman, yes. We do agree with you. The pipeline security guidelines which were published in 2011, and as you know, were a product of the collaboration with our security partners and our Federal partners, and we are in the process of updating those guidelines right now. We have already started the process. The process, though, is a collaborative one.

So we will be continuing our work with our security partners in the pipeline industry. So that work has already started. We have already started looking at the cyber portions, as a matter of fact, and we will be continuing that work so that we have an updated version of those guidelines.

Mr. KATKO. Okay. Thank you. Also now with respect to the actionable information and use of it, and proper use of it, I presume that oftentimes TSA gets information from the secret side.

I want to—you know, anybody can chime in here. I just want to make sure that we have the right mechanisms in place. If we don't now, what do we need to put those mechanisms in place so that the private sector can be briefed in properly about what the nature of those threats are without wrongfully disclosing the sensitive information. But we can't have this gulf, I don't think, where we have this information but we can't tell them about it.

So anyone care to address that? I would be happy to hear it.

Ms. JUDGE. Yeah. There are several operators that do hold secret clearances. Clearances are either issued—are either sponsored by TSA themselves. Some of our clearances are through DHS infrastructure protection. Some are from the FBI, and some are from Department of Energy. At last check there appeared to be over 300 clearance holders in the oil and natural gas sectors as of a little while back.

Mr. KATKO. But we do have 3,000 companies involved. So that is—might be a small percentage overall. So how do we—is that adequate, the number of people with the clearances to get this information?

Ms. JUDGE. It would depend on how many people from each—you know, are we covering each company's—each sector in the industry well enough? That I wouldn't be able to answer.

Mr. KATKO. Okay.

Ms. JUDGE. I know, for example, we have 3 clearance holders just at my company, 1 physical, 1 cyber, and 1 executive.

Mr. KATKO. Okay.

Ms. PROCTOR. Mr. Chairman, it would certainly depend on the nature of the information. If the information is specific, we would ensure that the appropriate systems are briefed on that information. If we need to get a tear line on that information, we will do that. We will ensure that if there is actionable information, that that information gets to the people who need to have it.

We do have a process with our Office of Intelligence and Analysis to ensure that the briefings occur wherever they need to occur across the country. We have field intelligence officers that are located at our airports. We have relationships with the FBI field offices or for those who are in the vicinity of the National Capital Region, we can ensure that they are appropriately briefed at TSA headquarters. So we have ensured that we have the ability to brief wherever that brief needs to be conducted.

Mr. KATKO. Thank you very much. My time has expired, but I will maybe come back to some of these questions.

The Chair now recognizes Ranking Member Rice for 5 minutes of questions.

Miss RICE. Thank you, Mr. Chairman.

I think I will ask Mr. Black, I guess start with you. There is—actually, I should say your study, Mr. Parfomak, there is a paragraph that is pretty small in comparison to the rest of the report talking about cybersecurity risks. The last statement ends with the statement that there is a suggestion that cybersecurity threats to pipelines have been increasing. So what specifically has the industry, both private and public, been doing to address this issue?

Mr. BLACK. Well, Dr. Parfomak mentioned rightly there is a great concern about cyber, about being prepared for cyber releases—cyber attacks. Excuse me.

The first element is this API standard on pipeline's data security. You have to keep your control system completely separate and apart from any business system that uses the internet. Then there is a number of Government programs that we participate in with industry. There is the FBI's InfraGuard process which is dedicated to sharing information. There is the NIST cybersecurity framework roadmap, and the—generally the ICS Cert process, the industrial control system Cyber Emergency Response Team, a partnership dealing with identifying threats, talking about how to prevent them. Then also talking about how to recover from those.

A couple of other API recommended practices. So cyber is on the minds of many of our members. When I asked in anticipation of this hearing what is the No. 1 security issue that you are thinking about, cyber is what I got. So it is on the minds of our security professionals.

Miss RICE. So when they say that, what do they give by way of example as to why that is their No. 1 concern? Is there enough—and I am not asking you to release any—or talk in this public setting about any kind of confidential or, you know, confidential information, but what——

Mr. BLACK. Well, in this space I think we are very aware of nation states and private actors trying to penetrate control systems and business systems. Oil and gas and beyond oil and gas. So that is something that we are focusing on. I can make sure that you get a Classified briefing on that or maybe that is a question for Director Proctor.

Miss RICE. Well, my question is, is it a—you know, we talk about having to stay 2 steps ahead. Right? Is it a technology issue? Is it a resource issue? I mean, what is the biggest challenge to ensuring that we are doing everything that we can because this cybersecurity is—I mean, obviously, as noted in this report, is an area of great concern. It just doesn't sound like there is—unless there is and you can't talk about it publicly. I get too, but——

Mr. BLACK. The threats are evolving and evolving quickly. So the industry and Government have to evolve and evolve quickly in terms of adapting to this. That is what these information-sharing programs are about. Thankfully it is not a prescriptive regulation that is outdated. This is real-time sharing of information, Government, what they are seeing, and industry personnel together discussing best practices. They might compete on commercial issues, but the industry can collaborate very heavily on safety and security. And they do.

Miss RICE. There is no obstacle to that? They are—because, I mean, I think everyone understands that it is in everyone's interest to have the same—the best technology, the best controls in place.

Mr. BLACK. Absolutely. Yes.

Miss RICE. So the informational sharing, with your Governmental partners, do you think that that is accurate? I mean, do you think that they give you accurate information, or do they—do you think that they withhold any information? Are there any issues related to information sharing that need to be addressed?

Mr. BLACK. I am not hearing of any concern. I am hearing that the Government personnel that are working on these issues are very well tied into the threats and the ways to address them. I hear a successful collaboration.

Miss RICE. Great. Thank you. I yield back the balance of my time.

Mr. KATKO. Thank you, Miss Rice.

The Chair now recognizes the gentleman from Georgia, Mr. Carter for 5 minutes of questioning.

Mr. CARTER. Thank you, Mr. Chairman. Thank each of you for being here. This is extremely important.

Ms. Proctor, I will start with you. I wanted to ask you, it is my understanding that TSA measures the risk to pipelines based on the amount of energy that is transported. Is that correct?

Ms. PROCTOR. Yes, sir. That is one of the criteria.

Mr. CARTER. What are the other criteria? I am sure the type of energy that it is or——

Ms. PROCTOR. We also look at the number of miles in high-consequence areas, which are designated by PHMSA. We look at the number of pipeline miles in high-threat urban areas, which are designated by DHS. We look at those pipelines that serve military bases, that serve the Department of Energy strategic petroleum reserves. We look at those that serve electric power plants. So there—the energy throughput is not the only consideration.

Mr. CARTER. But it is one of the primary ones?

Ms. PROCTOR. It is one. Yes, sir.

Mr. CARTER. Yes. Well, let me ask you. After that is done, then the operators identify critical facilities based on what is called the pipeline security guidelines. Is that correct?

Ms. PROCTOR. Yes, sir.

Mr. CARTER. What is done after that? After the pipeline owners identify those critical facilities, what happens after that?

Ms. PROCTOR. TSA then schedules reviews of the facilities. So we have identified the top 100 or so most critical pipeline systems by those criteria that we just named; the energy throughput, their pipeline mileage in the high-threat urban areas, and in the high-consequence areas. We go out and conduct assessments on-site.

Corporate security reviews are conducted at the pipeline headquarters where they review the actual corporate security plan. They conduct interviews of key security personnel on site. They also determine the extent to which the system is adhering to the agreed-upon process in the pipeline security guidelines.

Mr. CARTER. Okay. So they are essentially trying to mitigate as much risk as they can.

Ms. PROCTOR. Yes, sir.

Mr. CARTER. Okay. Let me move on. Ms. Judge, Mr. Black, I will direct these toward you-all. Do you feel like the biggest threats that the pipeline owners are facing right now, that they have been identified by TSA, they have changed any? Are they still the same?

Mr. BLACK. Correct.

Mr. CARTER. So you would feel like it is up-to-date as far as the biggest threats go?

Mr. BLACK. Right. It is physical and cyber and all different types of threats. The last security guidelines were issued in 2011, but what I hear consistently is that it is not static, is that the know-how and the information sharing and the intel that we get from TSA and our Federal partners is constantly evolving. It is 2016. It is——

Mr. CARTER. You are updating them as you go along as well?

Mr. BLACK. Yes.

Mr. CARTER. Okay. I want to ask you about—do you feel like that industry has gotten the tools that they need in order to mitigate as many risks as they can? Do you feel like there is anything else we could be doing to assist them?

Ms. JUDGE. I believe we have the tools we need. If we realize—we come along and we are like—we realize that there is something we may need, we just reach out, and usually they are more than happy to—you know, we would like a briefing on 1, 2, 3. They arrange to give us a briefing on 1, 2, 3. So there is that constant open communication through both one-on-one and through the sector coordinating councils, through the security committees that——

Mr. CARTER. Okay.

Ms. JUDGE [continuing]. When we express needs, we usually get what we need.

Mr. CARTER. Well, let me ask you collaboration. Because that is extremely important. Do you ever give security clearance to any of these pipeline companies, to any of their personnel to possibly share any kind of threats with them that you might have heard of?

Mr. BLACK. They have Classified and Unclassified briefings on these TSA pipeline security calls. There is some For-Official-Use-Only information that is in Unclassified settings that you can get to more people. Some things have to be shared only in a Classified briefing, and they are.

Mr. CARTER. Okay. So you would rate the collaboration as being good at this point?

Mr. BLACK. Yes.

Mr. CARTER. Okay. I am sorry. I can't—the glare is too bad, Dr. Parfomak. Would you agree with that?

Mr. PARFOMAK. Excuse me. Could you repeat the question?

Mr. CARTER. Would you agree that the collaboration between private industry and TSA has been good?

Mr. PARFOMAK. As I mentioned in my opening statement, CRS doesn't advocate policy or take a position on that. Whether the collaboration has been good, as I said in my opening statement, is a debatable point. Others have raised the issue of, for instance, DOT's and TSA's collaboration, and that may have been evolving over the last number of years.

Mr. CARTER. Okay. Well, obviously, you-all understand how important collaboration is. So I would certainly hope we are making a concerted effort at doing the best we can with that.

Thank you, Mr. Chairman.

Mr. KATKO. Thank you, Mr. Carter.

The Chair now recognizes the gentleman from Texas, Mr. Ratcliffe, for 5 minutes of questioning.

Mr. RATCLIFFE. Thank you, Mr. Chairman, Ranking Member.

This is an important hearing today, not just for the country but particularly my home State of Texas. Texas has the largest pipeline infrastructure in the Nation, more than 425,000 miles of pipeline in our State, which is roughly, I believe, one-sixth of the total pipeline mileage in the United States. Many of those pipelines do actually run through the Fourth Congressional District that I am privileged to represent.

So I appreciate all of you being here today to talk about the ongoing efforts to secure our pipeline infrastructure and what can be done to enhance the partnership between TSA and industry.

Director Proctor, in your written testimony you referenced the recent attacks in Brussels to illustrate the fact that terrorist threats have grown incredibly complex, we know that, and that terrorist actors can become radicalized to carry out these attacks with little or no warning. I agree with your assessment of the current threats posed by these terrorists. I was also pleased to hear that TSA and the pipeline industry have a good working relationship to protect our critical infrastructure.

I am curious, though, with roughly 3,000 private companies who own and operate the Nation's pipelines, how does TSA communicate threat assessments to these companies and recommend improved measures in the wake of potential threats made against a specific pipeline?

Ms. PROCTOR. Thank you for that question.

Our Office of Intelligence and Analysis conducts an assessment, an annual assessment, of the threats to the pipeline industry. One of those assessments is an Unclassified assessment that we can share with industry. We do share that. We share that with the pipeline industry and we continually communicate information that we get from our intelligence and analysis office if there is any information that could indicate a possible threat, a generalized threat.

If it is a specific threat and it is Classified information, we arrange for a Classified briefing with that particular entity. We do have the means to do that through our partners either with the FBI at a local field office, with a field intelligence officer at an airport, or through a meeting at TSA headquarters. We can provide Classified information.

Mr. RATCLIFFE. So in addition to the briefing, though, in a Classified setting, are you making specific recommendations? If so, are you finding that industry is receptive to those?

Ms. PROCTOR. We do make specific recommendations. We conduct both corporate security reviews and critical facility security reviews. At the conclusion of that review, and they are done on-site at the pipeline facility, there are recommendations, if it is appropriate, there are recommendations that are made and provided to the security director of the pipeline organization. They are provided at the time. They are followed up with written recommendations.

So we do those on-site assessments and provide those recommendations that are specific to that company. We provide more generalized recommendations for security in our monthly conference calls or calls that may be generated by some issue that has occurred in the news. If we feel it appropriate, we will have a conference call just to share information that we have, and to share any recommendations that we think would help enhance the security in the pipeline industry.

Mr. RATCLIFFE. Thank you. Very quickly, I want to move to the industry side, because I know Mr. Black, Ms. Judge, that, you know, with the evolution of technology and the need to keep your technology updated to protect infrastructure from bad actors, I am curious about your perspectives on the partnership between TSA and industry in advancing proactive security measures.

Specifically I want your perspectives on whether TSA, from your, again, perspective, is timely sharing cyber threat information and intelligence information in such a way that is allowing you to bolster your defenses against these threats?

Mr. BLACK. From liquids pipelines, I am not hearing any concerns about timeliness. I am hearing that, just as you and Director Proctor discussed, that we get company-specific guidance on company-specific issues. The concern that I am hearing is the TSA has some important vacancies in the pipeline security division that need to be filled. We are looking forward to those being filled with good quality people so that we can have more people to collaborate with.

Mr. RATCLIFFE. Great. Ms. Judge, do you want to weigh in?

Ms. JUDGE. Yes. We haven't heard of any in the natural gas pipeline side of things not getting timely information. We actually get very timely information, oftentimes from several different departments and at the same time. So we are getting timely information sometimes 3 or 4 times being the same information. So no issues there.

Mr. RATCLIFFE. Okay. Well. My time has expired, but if the Chairman will indulge just very quickly, because I want to give you an opportunity, and maybe this has been asked. But if you could alter the relationship between TSA and industry in one specific way or a specific way to better secure our pipeline infrastructure, what change would you recommend?

Ms. JUDGE. As of this minute, the one change I would make would be to fill, as Andy said, fill the open positions so that we can start collaborating more closely again with whomever is coming in. Part of that is, as Sonya said, we are currently reviewing the pipeline guidelines, and that is a collaborative effort with TSA and with the industry through the Pipeline Sector Coordinating Council. It would be really great once they do hire and on-board the new replacement for the head of this group, we can, you know, work real closely with them to get these guidelines updated and get them out there so people can implement any changes they need to.

Mr. RATCLIFFE. Terrific. Thank you.

Mr. BLACK. It is people. It is leadership roles that have been filled that—we would be remiss if we didn't praise Jack Fox who recently retired from TSA. That is big shoes to fill. Jack did a nice job at helping us all be focused on pipeline security. If they can find the right type of people to succeed Jack and a couple of the other positions, we will be better off and ready to collaborate more intensely.

Mr. RATCLIFFE. Terrific. Thank you all for being here. Chairman, thanks for your indulgence.

Mr. KATKO. Thank you. Excellent questions. Thank you, Mr. Ratcliffe.

All right. I just have few more questions, and of course any of my other colleagues that are here can follow up if they wish.

With respect to resources—I want to follow—what is the reason, Ms. Proctor, for some of those openings? How—when do you plan on filling them?

Ms. PROCTOR. Mr. Chairman, we have recently had the retirement of Mr. Jack Fox, the long-time manager and leader of our pipeline office. They are very big shoes to fill. We recognize the importance of having industry experience in our pipeline office. So we have recruited heavily from the industry. I am very happy to say that I have interviews scheduled in the next week to actually make a selection on the position for the manager of our pipeline office.

The other positions that we have there have been posted. I have received Cert lists on those. We have interviews that are being scheduled for those. So we will have a full house in our pipeline section.

Mr. KATKO. Okay. How long have those positions been open?

Ms. PROCTOR. Mr. Fox actually retired in February. One other gentleman just left last month. So they are fairly recent.

Mr. KATKO. Okay. Now that kind of bleeds into my next concern. That is what Dr. Parfomak pointed out, and that was potential for resource issues. Now, a fiscal conservative like me and someone who likes smaller government, it is troublesome to ask a question like this. But do you need more resources?

Ms. PROCTOR. Mr. Chairman, I don't know anyone who wouldn't——

Mr. KATKO. Such an easy question. Oh my gosh.

Ms. PROCTOR [continuing]. Who wouldn't acknowledge loving more resources. Certainly if those resources were available, we would invest them and put them to good use. We would invest in additional training with our pipeline industry partners, and we would also invest in conducting additional assessments at critical facilities.

Mr. KATKO. Do you have in mind what exactly the type of positions you would like to enhance? Do you have a plan as to what you would do with the additional resources that we could look at and assess?

Ms. PROCTOR. I could certainly provide that, Mr. Chairman.

Mr. KATKO. I would appreciate that. I would like to take a look at that. Because I think that, you know, with the emerging threat, it may be when you are updating your 2011 guidelines, that might impact your thought process too. So perhaps when you submit those, I would like to see those, maybe we can have an update as to what you think you could do if you had additional resources and why you need the additional resources. That would be helpful. I would appreciate input from the industry as well on that.

Now, most of the guidelines and suggestions you issue on the security side are voluntary. Is that correct?

Ms. PROCTOR. Yes, Mr. Chairman, they are voluntary.

Mr. KATKO. Okay. Now, the cynic in me would say that is why the industry likes you so much. Because they are voluntary, not mandatory. So would it be helpful to have some of those things—or do you ever find any frustration, I should say, with issuing guidelines and them not following them, and then you think it is really important for them to do so?

Ms. PROCTOR. No, sir. I believe the environment in which we operate now allows a great deal of flexibility. Certainly in the current environment with the evolving threats, the ability to be flexible I think is very important. We have had great success with voluntary guidelines. We have not had any pipeline industry partners to balk at complying with the guidelines that we have agreed upon. So we are pleased to have this kind of collaboration and this partnership with the industry. It allows us to have open discussion, and it allows us to work in a collaborative way to solutions. So we are very pleased with the arrangement.

Mr. KATKO. I must say in going through this hearing and, again, preparing for this hearing as well and talking to some of the individuals who were going to testify that the spirit of public/private cooperation is encouraging. I am a very big advocate of the private sector working collaboratively with the Government instead of at odds with them. It helps us leverage the finite Government resources that we have.

So I applaud all of you for working collaboratively together. It is very important. In this age of budget constraints, the private sector has to play a role. It is an increasingly important role. I don't think we should ever be in a situation where the Government is telling industry what to do. That is when we have problems. It seems like more collaboration here is a very good thing. I applaud all of you for what you are doing in keeping our country safe with respect to that.

If you have additional input you want to provide, some things you wish we asked you today, please feel free to do so. Please get it to us because we will listen and we will take a look at it. But this seems like an area, unlike many other areas we have oversight of with respect to TSA, that this seems to be working pretty well. I am happy to say that.

So in accordance with our committee rules and practice, I plan to recognize—oh, excuse me. All done with that. Pardon me.

I do want to thank the panel for the thoughtful testimony. Members of the committee may have some additional questions for the record. We ask that you respond to those in writing.

The hearing record will stay open for 10 days. Without objection the subcommittee stands adjourned.

[Whereupon, at 3:24 p.m., the subcommittee was adjourned.]

# APPENDIX

---

## QUESTIONS FROM RANKING MEMBER BENNIE G. THOMPSON FOR SONYA PROCTOR

*Question 1.* Given that pipeline systems are within the Transportation System sector, one of the 16 critical infrastructure sectors under PPD–21, and that these pipelines often depend on computer and communications networks used for automated control, please describe, with specificity, what type of coordination, if any, there is between TSA and National Protection and Program Directorate to strengthen and make more resilient this critical infrastructure.

Answer. Response was not received at the time of publication.

*Question 2.* NPPD has a network of Protective Service Advisors across the country who are charged with proactively engaging with the private sector to protect critical infrastructure.

Does your office work with the network of PSAs?

Answer. Response was not received at the time of publication.

*Question 3.* Does TSA or NPPD provide training programs to private industry employees that provide security certifications? If so, please elaborate.

Answer. Response was not received at the time of publication.

*Question 4a.* In the planning phases of a pipeline system project, what role, if any, does TSA play in decision making regarding security concerns that may arise?

*Question 4b.* To your knowledge, are any other agencies involved in making security decisions during the planning phases of pipelines?

Answer. Response was not received at the time of publication.

*Question 5a.* Your testimony states that TSA works closely with DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA). PHMSA handles the safety aspect of pipelines, while TSA handles the security aspect.

*Question 5b.* Since safety and security are closely associated, could you detail for us how TSA works with PHMSA to address both issues?

Answer. Response was not received at the time of publication.

*Question 6.* Ms. Proctor, please detail TSA's role in providing guidelines to industry for individuals seeking positions with unrestricted access at critical pipeline assets.

Answer. Response was not received at the time of publication.

*Question 7.* TSA has regulatory authority over pipeline systems for purposes of security. To date, TSA has not exercised this authority.

How often do you evaluate the security risk to these systems and do you have internal criteria for what might trigger regulatory action?

Answer. Response was not received at the time of publication.

*Question 8.* As among the various security risks to pipeline systems, where does interference with SCADA control systems factor?

Do you have risk-modeling to understand what cascading effects may be triggered by a cyber or physical attack on a pipeline?

Answer. Response was not received at the time of publication.

*Question 9a.* When are they updating the 2 key 2011 documents and what changes should we expect to see?

*Question 9b.* Will protection of control systems factor be more prominent?

Answer. Response was not received at the time of publication.

## QUESTION FROM RANKING MEMBER BENNIE G. THOMPSON FOR KATHLEEN S. JUDGE

*Question.* Ms. Judge, in your testimony you stated that gas companies work closely with law enforcement personnel and first responders on site-specific plans and security drills.

How often do these security plans and security drills take place, and how often are these plans updated?

Answer. The question posed relates to how often security plans are updated and how often security drills take place. Corporate Security Plans are typically reviewed annually and updated as required and as circumstances warrant. Site-Specific Plans include measures tailored for each specific critical facility and include specific actions to be taken at the elevated and imminent levels of the National Terrorism Alert System. As stated in the TSA Pipeline Security Guidelines these plans should be reviewed and updated on a periodic basis, not to exceed 18 months. As threats evolve, so does security. Typically there is one major security drill or exercise per year. Also, periodic security drills or exercises are performed either independently or in conjunction with other regularly-scheduled required company drills or exercises.

## QUESTIONS FROM RANKING MEMBER BENNIE G. THOMPSON FOR PAUL W. PARFOMAK

*Question 1.* When we think of possible attacks on all sectors, we often quantify the damage in terms of the potential loss of life. Throughout testimony, we saw repeatedly that the consequences of an attack on our Nation's pipeline systems could cause severe consequences to our economy, environment, as well as the loss of human life. Would you please explain to us the possible effects of an attack on our pipeline systems in regard to these 3 factors?

Answer. Because energy pipelines carry volatile, flammable, or toxic materials, they have the potential to cause public injury, economic damage, and environmental damage in the event of an uncontrolled release—be it the result of an accident or deliberate attack. The nature and severity of such consequences in any particular incident depend upon many factors, including the product involved, the scale of the release, proximity to a population or environmentally-sensitive area, the emergency response, and other factors. For example, a natural gas release may present a greater risk to people than crude oil because it is more volatile, but it presents less environmental risk because it burns off quickly or dissipates in air. Crude oil, on the other hand, may cause much more extensive environmental harm, particularly when released into water where it can spread quickly. Nonetheless, crude oil may still cause personal injury, especially if it ignites. The economic impacts of any pipeline release involve both damages in the vicinity of the incident and damages due to lost commodity and to disruption of the pipeline supplies to customers that depend upon them—such as power plants, factories, and refineries.

As I stated in my written testimony, although there have been no successful terrorist attacks on pipelines in the United States, notable safety incidents over the last 15 years or so illustrate the potential damages from uncontrolled releases.

- *1999*.—A gasoline pipeline explosion in Bellingham, Washington, killed 3 people and caused $45 million in damage to a city water plant and other property.
- *2000*.—A natural gas pipeline explosion near Carlsbad, New Mexico killed 12 campers.
- *2006*.—Pipelines on the North Slope of Alaska leaked over 200,000 gallons of crude oil in an environmentally-sensitive area and temporarily shut down Prudhoe Bay oil production.
- *2007*.—A release from a propane pipeline near Carmichael, Mississippi killed 2 people, injured several others, destroyed 4 homes, and burned over 70 acres of land.
- *2010*.—A pipeline spill in Marshall, Michigan released 819,000 gallons of crude oil into a tributary of the Kalamazoo River. Expenses to clean up the spill exceeded $1.2 billion. The pipeline operator also lost $16 million in revenue while the line was out of service.
- *2010*.—A natural gas pipeline explosion in San Bruno, California, killed 8 people, injured 60 others, and destroyed 37 homes. California regulators imposed on the operator a fine, penalties, and other remedies totaling $1.6 billion.
- *2011*.—A natural gas pipeline explosion in Allentown, PA, killed 5 people, damaged 50 buildings, and caused 500 people to be evacuated.
- *2011*.—A pipeline spill near Laurel, MT, released an estimated 42,000 gallons of crude oil into the Yellowstone River.
- *2014*.—A natural gas distribution pipeline explosion in New York City killed 8 people, injured 50 others, destroyed 2 5-story buildings, and caused the temporary closure of a transit line due to debris.
- *2015*.—A pipeline in Santa Barbara County, CA, spilled 143,000 gallons of crude oil, including 21,000 gallons reaching Refugio State Beach on the Pacific Ocean.

These incidents may have imposed additional economic damages among pipeline users to the temporary disruption of pipeline supplies, but such "downstream" economic impacts are generally not quantified in accident investigations.

*Question 2.* It seems as though a wide array of Government actors have responsibilities regarding the safety of pipelines. In your view, are there any areas of overlap or redundancy in the Government's efforts to ensure that pipelines are secure?

Answer. Three Federal agencies play the most significant roles in the formulation, administration, and oversight of pipeline safety regulations in the United States. The Department of Transportation's (DOT) Pipeline and Hazardous Materials Safety Administration (PHMSA) has the primary responsibility for the promulgation and enforcement of Federal pipeline safety standards. PHMSA regulates key aspects of safety for energy product pipelines in the United States: Design, construction, operation and maintenance, and spill response planning (see Title 49 of the Code of Federal Regulations). PHMSA's enabling legislation also allows the agency to delegate authority to intra-State pipeline safety offices, and allows State offices to act as "agents" administering inter-State pipeline safety programs (excluding enforcement) for those sections of inter-State pipelines within their boundaries. The Federal Energy Regulatory Commission is not operationally involved in pipeline safety, but it examines safety issues under its siting authority for inter-State natural gas pipelines. The National Transportation Safety Board investigates transportation accidents—including pipeline accidents—and issues associated safety recommendations.

As stated in my written testimony, Federal oversight of pipeline security falls under the jurisdiction of the Transportation Security Administration (TSA) within the Department of Homeland Security. Although the TSA has regulatory authority for pipeline security, its activities rely upon voluntary industry compliance with the agency's security guidance and best practice recommendations.

Since TSA was established, Congress has had a continuing interest in the appropriate division of pipeline security authority between the DOT and TSA. In 2004, the DOT and DHS entered into a memorandum of understanding (MOU) concerning their respective security roles in all modes of transportation. The MOU notes that DHS has the primary responsibility for transportation security with support from the DOT, and establishes a general framework for cooperation and coordination. On August 9, 2006, the Congressional Research Service departments signed an annex "to delineate clear lines of authority and responsibility and promote communications, efficiency, and nonduplication of effort through cooperation and collaboration between the parties in the area of transportation security."[1] According to TSA, the 2 agencies maintain daily contact, share information in a timely manner, and collaborate on security guidelines and incident response planning. Although pipeline safety and security, in some cases, may be operationally related, CRS is not aware of any recent reports or industry comments suggesting that there is overlap or redundancy between TSA's activities in pipeline security and PHMSA's activities in pipeline safety.

○

---

[1] Transportation Security Administration and Pipelines and Hazardous Materials Safety Administration, "Transportation Security Administration and Pipelines and Hazardous Materials Safety Administration Cooperation on Pipelines and Hazardous Materials Transportation Security," August 9, 2006.