This publication is part of the Deloitte Center for Regulatory Strategy, Americas cross-industry series on the year’s top regulatory trends. This annual series provides a forward look at some of the regulatory issues we anticipate will have a significant impact on the market and our clients’ businesses in 2019. The issues outlined in each of the reports provide a starting point for an important dialogue about future regulatory challenges and opportunities to help executives stay ahead of evolving requirements and trends. For 2019, we provide our regulatory perspectives on the following industries and sectors: banking; capital markets; insurance; investment management; energy, resources, & industrials; life sciences and health care.

We hope you find this document to be helpful as you plan for 2019 and the regulatory changes it may bring. Please feel free to contact us with questions and feedback at CenterRegulatoryStrategyAmericas@deloitte.com.
# Contents

**Introduction**  
Operational integrity and safety  
The digital future of compliance  
NERC  
Cybersecurity  
Regulatory process  
Know Your Counterparty  
De minimis threshold for swaps  

**Endnotes**  
**Contacts**
Introduction

In this Fifth Annual Energy Regulatory Outlook, Deloitte's Center for Regulatory Strategy has identified seven priority areas for 2019.

1. Operational integrity and safety
2. Digital future of compliance
3. North American Electric Reliability Corporation (NERC) trends
4. Cybersecurity and privacy regulations
5. Regulatory process
6. Know your counterparty
7. Commodities Futures Trading Commission (CFTC) de minimis value for swaps portfolios

Typically, it is relatively easier for legislators and regulators to refine regulations, as compared to establishing or eliminating new ones. The exception is using executive authority to create rules with or without the support of Congress, which is a relatively recent practice that can be controversial.

Regulations can be refined in a variety of ways: passing new legislation; cutting funding and/or staff in key areas; appointing new leadership that opposes the regulations; changing technical standards and/or limiting a regulatory body's ability to conduct technical and scientific research; or simply choosing not to enforce the rules.

In response to reduced regulation at the federal level, some states are developing their own statutory solutions to help fill the void. These state-level policies could ultimately have a national impact, particularly if states leading the charge such as California with its renewable energy requirements and other efforts persist in this approach and can set a path for others to follow.

Also, at both the state and federal levels, there is a growing use of judicial challenges by political activists, such as those challenging the expansion of coal assets. Although this tactic tends to be more impactful for new regulations (as opposed to existing regulations that are now simply being enforced in a different manner); such challenges are likely to continue. Either way, however, their effectiveness and impact may not be understood or felt for years as the rulings crawl through the appellate process, which itself may be shaped in uncertain ways by federal judicial appointments.

The recent midterm election results have created the potential for a more static environment when it comes to legislative or regulatory change with the split houses of Congress; consequently, at this point, significant near-term change for the energy industry seems unlikely. Regardless of what definitive changes lawmakers and regulators might make, energy organizations should continue to drive effectiveness and efficiencies across their risk and compliance programs while closely monitoring the regulatory landscape for definitive signs of developing trends that could bring meaningful and lasting change.
For regulators that oversee physical infrastructure, there is an increasing focus on the safety, integrity, and reliability of the operations associated with that infrastructure. This is true whether the regulator oversees power plants and transmission lines (e.g., Federal Energy Regulatory Commission [FERC] and NERC), or natural gas pipelines and liquefied natural gas facilities (e.g., Pipeline and Hazardous Materials Safety Administration [PHMSA] and state utility commissions).

Actual events and incidents—as well as near-misses—whether widely publicized or addressed more discreetly, have increased the attention companies are placing on the rigor of their compliance oversight practices. This includes capturing data and records that help them demonstrate the monitoring, maintenance, and remediation practices they are following to meet their own standards and those set by regulators.

High-profile incidents related to pipelines, liquefied natural gas plants, power plants, and electric transmission infrastructure have further heightened companies’ awareness of tactical activities and practices such as records management and information governance, continuous controls monitoring, performance management, training development and delivery, and reinforcement of corporate culture and employee behavior.

Regulatory compliance expectations are rising from every source—regulators, shareholders, boards of directors, executive leadership, counterparties, and even customers. In response, a growing number of companies are starting to take a close look at the lessons that can be learned from these events, whether or not they were directly involved. The main question they are asking themselves is: “Could it happen here?”

Companies want to ensure that the operational integrity of their assets—and the safety of their employees, contractors, vendors, and customers—is maintained at a high standard. Also, there seems to be increasing awareness that strong safety and compliance practices can yield better overall returns for shareholders. To those ends, many companies are either developing or reexamining their compliance and risk self-assessment programs as a strong first line of defense against potential incidents or events that could disrupt operations, damage assets, or harm people.

These shifts in the industry are not the result of new regulations; rather, they are a response to actual market and/or operations events that have triggered intense regulatory scrutiny. Such events are prompting regulators across North America to scrutinize the operational integrity management practices of the companies they oversee—causing them to question what is in place, whether it is sustainable, and if companies are adhering to their own stated practices and policies.

Regardless of how a company has responded to these kinds of industry events in the past, boards and regulators now expect organizations to have a solid first line of defense that includes compliance and risk self-assessment practices, along with substantive programs that enable them to adequately monitor themselves for compliance.

Assurance professionals have long espoused the mantra of “trust but verify.” However, this approach is now also becoming a standard principle for frontline supervisors and managers within operating units. It is no longer acceptable for organizations to rely solely on the compliance, risk, and internal audit functions to carry the lion’s share of the burden for protecting an organization against events that could jeopardize safety, integrity, or reliability. More recently, with organizations that live this approach, the leading practice is to make compliance risk management an integral part of the culture and weave it into day-to-day business processes, rather than treating it as a separate activity.

What do leading-class compliance and risk self-assessment capabilities look like? First and foremost, regulatory requirements and/or industry standards applicable to the company are explicitly documented. Second, an agreed-upon operating model is in place that addresses the roles, responsibilities, expected control activities, and cadence for each of the identified self-assessment activities. Third, findings and observations from the assessments are captured in a report—with ongoing tracking of the corrective actions necessary to further strengthen the control environment for the organization’s first line of defense. These findings are, in turn, socialized across their respective organizations to foster a continuous improvement philosophy.

Although there is much more that goes into creating a robust program for managing compliance risk, the three areas above are a foundation for what many regulators expect companies to have in place today.
The digital future of compliance

Broadly speaking, corporate stakeholders are demanding a greater focus on embracing digital technologies. In the context of the regulatory environment, digital initiatives are creating more robust mechanisms that help protect business value and enable energy companies to proactively identify and remediate potential regulatory issues that might otherwise lead to fines and brand damage. Although the energy industry has typically trailed others in the area of digital innovation, many energy companies are now taking significant steps to identify and assess opportunities to add business value by leveraging technology within a well-defined strategic framework.

Recent digital advances in the energy industry have largely been driven by pressure from executive leadership to cut costs and save time during a period of low commodity prices. Successful pilot initiatives have increased confidence that investing in digital innovation can deliver a tangible return on investment. The role of digital technologies is expanding rapidly in energy and there are numerous opportunities to piggyback on early successes by using existing technologies and readily available data to strengthen regulatory compliance frameworks. Automation, natural language processing/generation, advanced analytics, data visualization, and blockchain are some of the primary technologies experiencing wider adoption. Technologies like these are currently being used to monitor multiple data sources and inform companies when compliance issues may be lurking.

The expanded use of digital technology within energy will continue to impact the way businesses operate in the future, and may ultimately change the relationship between regulators and the business community. Currently, the increased ability to perform deeper analysis—and the broadening application of data science capabilities—is helping energy companies shift from being “risk-aware” to “risk-prepared.” Companies are using predictive risk intelligence technology to scan thousands of media sources looking for third-party behavior that may create regulatory risk. Advanced analytics are being used to detect fraud, waste, and abuse in a structured and time-efficient manner that enables proactive identification and remediation.

Moving forward, energy companies need to determine how their workforces will be affected by the impacts of advanced technologies and increasingly complex regulatory demands. Digital advancement in the energy industry will almost certainly continue. Also, business functions that can benefit from technology advancement will increase in breadth and depth in areas such as health and safety, counterparty/customer relations and contract compliance, environmental management, and employee/contractor training and education. At the same time, regulatory pressures will presumably be on the rise, with regulators expecting greater transparency and shorter response and remediation timelines.

Although digital improvements will likely positively affect the way energy businesses operate, new risks will accompany these improvements, necessitating greater communication across siloed functions, along with more robust governance models to manage the risks associated with increased reliance on technology. On the other hand, increased adoption of technology presents an opportunity for leadership teams to be thoughtful about how to foster the cultural changes necessary for future success.

To capitalize on the potential benefits of the digital wave that is already in motion, energy companies should first seek to understand where they currently fall on the digital continuum—and then decide where they want to be. In so doing, it will be critical to develop a strategic future-state vision that is fit for purpose, and then build upon existing use cases to outline a path forward.

Here are some important practices that can help a company effectively embrace digital technology as part of its regulatory strategy:

- **Establish a strong change management framework.** Given the exponential rate of technology innovation, the journey to embracing a digitally enabled future will likely be highly dynamic and fast-paced. Without strong change management, employees can get left behind and disengage from the process.

- **Create a continuous feedback loop.** Document the lessons learned from pilot programs and continuously strive for large-scale adoption. Also, in an ever-evolving environment, elements of digital roadmaps will become quickly outdated and need to be adjusted along the way.

- **Develop leaders with the agility needed to embrace a digital future.** Identify and invest in top employees who can disrupt, lead, and exponentially evolve.

- **Help shape the future.** Digitally focused consortiums and industry groups are gaining influence. Consider getting a seat at these tables to have a voice as new standards are being shaped.

By managing digital adoption effectively, energy companies can elevate their stature with regulators, improve the efficiency and effectiveness of their regulatory change management, and focus more time on activities that are proactive and strategic. They can also transform and improve their processes in a way that increases shareholder confidence and protects business value.
More than 10 years have passed since the first of the NERC requirements became mandatory enforceable regulations. During that time, the industry tradition of continuous improvement has been applied to the rulemaking process for NERC regulatory standards, with each year bringing a slate of revisions to existing standards—and occasionally a few new ones. To ensure adequate engagement in the standards development process (and sufficient time to implement), continuous monitoring is essential.

This year, the biggest addition comes from the final approval of NERC Standard CIP-013-1—Cyber Security Supply Chain Risk Management. Other highlights include a few key enforcement trends, as well as the continued focus by entities on shifting their existing programs to risk-based program implementation approaches.

**CIP-013-1 Cyber Security Supply Chain Risk Management**

With the issuance of FERC Order 850, the NERC critical infrastructure protection (CIP) supply chain requirements are finally approved, and the industry’s focus can now formally shift to implementation. With an effective date of July 1, 2020, the Order provides 18 months for implementation and compliance, all of which will likely be needed, even for entities that had a head start.

CIP-013-1 is a risk-based standard that sets forth an obligation to “develop a plan and follow it.” Although this approach will be familiar to entities that implemented the early versions of the Order 693 operating standards, it is intended as a more mature risk-based approach than prior attempts. As such, it could be the first fully discretionary standard of this magnitude under today’s more structured, risk-based approach to enforcement. Also, while FERC provides enforcement guidance to NERC and the Regional Entities, there remains a broad landscape for regulators to challenge the entity approach, potentially creating uncertainty for many entities during the initial implementation effort. These potential concerns can be mitigated through sufficient advance planning and action, and through coordination with the applicable Regional Entity. A few highlights from the new standard include:

- The objective is to address supply chain-related cybersecurity risks (e.g., insertion of counterfeit components), and to improve defenses against attacks that are increasingly targeting supply chains (e.g., bulk electric system [BES] integrators).
- Most entities will initially implement the new standard by updating contractual language for third-party vendor goods and services and by adding some technical controls to ensure that the authenticity of goods can be verified and that third-party access can be managed more effectively.
- The standard also calls for the implementation of updates to third-party agreements on a going-forward basis and accounts for the challenge of implementing controls for existing agreements.
- A few gaps remain—such as the lack of adequate coverage for Electronic Access Control or Monitoring Systems (EACMS)—and FERC has explicitly required NERC to address these gaps in future iterations of the standard.

The standard will not take effect until July 1, 2020, and has incorporated much of the industry feedback to address some of the more significant challenges with implementing supply chain controls. However, a substantial amount of preparation may still be needed. Entities should assess the requirements and begin work on the transition immediately.
Enforcement trends
NERC is maintaining a rigorous approach to enforcement, and Regional Entities continue to leverage the various mechanisms at their disposal to ensure industry dedication to good compliance. Enforcement will likely continue to focus on NERC CIP compliance, and on operating standards that regulate the types of failures that contributed to larger-scale outages. Recently assessed penalties for facility ratings violations highlight one challenge that entities face when managing compliance to standards in situations where a large number of assets are in scope and/or complex or numerous activities are required to comply. Three primary focus areas where enforcement activity is likely are:

- **Vegetation management.** Prevention of program implementation complacency. Has adequate consideration been given to annual climate issues and trends affecting the program, including current-day events that may be accelerating vegetation growth?

- **Facility ratings.** Inclusion of all components, and accurate ratings of each component. Was the original rating process/methodology aligned to a good ratings methodology, and has this issue been evaluated as part of the now-regulated program?

- **Protection system programs.** Has all equipment been included in the program? Has adequate consideration been given to neighboring entities and shared equipment? Are processes in place to ensure proper vendor or contractor implementation of the program?

Shifting to a risk-based approach
Entities will likely continue working to transition their existing NERC programs to a mature risk-based model with processes and controls that more effectively incorporate a risk-based approach, while at the same time aligning with the NERC and Regional Entity approaches to risk-based standards and compliance enforcement. Many entities are pursuing this effort through a phased approach, and their programs will likely require continuous assessment as the standards evolve.
Cybersecurity is one of the most uncertain and rapidly changing regulatory areas for every industry. With the frenzied pace of technology change across all aspects of business operations—and the corresponding rise in attempted cyber intrusions and attacks—regulators are becoming increasingly concerned about cyber risks. The past year saw a significant increase in regulation of privacy and cybersecurity for many industries, with a major focus on data protection and supply chain. Looking ahead, risks and regulations in this area are likely to increase, and energy companies will need to position themselves for these changes sooner than they might have expected.

**Major trends in cybersecurity regulation**

The biggest news on the cybersecurity regulatory front for 2018 was the General Data Protection Regulation (GDPR).° GDPR primarily addresses data protections and privacy within the European Union (EU) and European Economic Area (EEA). However, it also addresses the export of personal data to areas beyond those jurisdictions, which greatly broadens its impact since many businesses around the world use websites and other tools that collect personal data from individuals in the EU and EEA.

For now, the full impact and implications of GDPR are still being assessed. While some global entities have completed an initial analysis and implementation, many are still grappling with myriad complex questions about the regulation’s applicability—particularly outside of the EU—and what enforcement of the rules will look like. New regulations of this scale often take several years to implement, as they tend to evolve over time. Although GDPR originated in the EU/EEA, some US regulators are beginning to issue similar rules. For example, California recently passed the California Consumer Privacy Act of 2018 (CCPA), which is scheduled to take effect in 2020. California’s privacy regulations are more limited than GDPR but include protections for minors, and thus far are the most comprehensive US-based regulations for this type of data. While California was the first state to act, entities can expect to see similar policy proposals over the next few years in other states (and possibly at the federal level).

Beyond GDPR applicability, the question of “who’s next” also remains. Regulators often take cues from other jurisdictions on potential policies within their own regions. The introduction of blockchain provides some potential ideas and opportunities for managing supply chain risk more effectively; however, many businesses do not know how to apply these solutions outside of the financial realm. Also, blockchain-related technologies and tools are still in the early stages of maturity and thus are not yet being meaningfully deployed in most industries.

Another important trend in 2018 was the growing linkage between IoT risks and ICS—particularly in critical infrastructure. While regulations are starting to address some aspects of operating technology (OT), the focus of regulators has not yet been on emerging IoT devices or ICS beyond those within the utility industry. Regulation of cyber activities and assets will continue to expand, but in the meantime, organizations should address this area when developing overarching long-term strategies for mitigating cybersecurity risk.

**A complex and expanding regulatory landscape**

Many industries have some form of applicable regulation in place for discrete business activities, such as customer information protections. Also, some domains, such as the BES, have their operations completely regulated to ensure protection of all critical cyber assets. In addition, most entities adhere to various industry frameworks (e.g., the National Institute of Standards and Technology [NIST]° and standards (e.g., ISO/IEC 27032°). However, as the focus and understanding of cyber risks grow both among regulators and consumers, more regulation is likely to come.
Beyond the anticipated additional regulation, the unique nature of cybersecurity introduces complex questions for regulators—particularly “who” regulates “what”? Where is the line between federal and state regulation, and in situations where several regulators may be involved, is it clear who plays what role? Many industries are regulated by several agencies at the federal level, each of which may arguably have jurisdiction—resulting in potentially confusing overlaps.

**Taking action**
With the increase in privacy and cybersecurity regulation—and rapidly expanding cyber risks—companies need to ensure they have an effective long-term strategy with greater focus on management of cybersecurity regulatory, operating, and compliance controls. Traditional approaches that are primarily tactical and reactive in nature are no longer sufficient.

A cross-functional capability is more important than ever, both for analyzing and designing a future cybersecurity strategy, and for the ongoing implementation and potential defense (if subject to regulatory scrutiny) of any cyber-related program. A collaborative role that combines legal and regulatory capabilities with stronger technical understanding is especially important.

Many entities are also recognizing that their traditional governance and compliance functions are not adequate for today’s landscape. Leading practices include the expansion of governance and compliance functions to explicitly focus on cybersecurity. Even if cyber and privacy regulations are not yet in place, organizations should consider focusing on those areas in new and expanded ways. For example, governance and compliance can play a critical role in ensuring processes and controls are being implemented as designed, thus helping to mitigate cyber risk.

Entities should start by making sure they have the right people and processes in place to monitor and implement any required changes. Many entities are beginning to include cybersecurity either within the purview of the chief compliance officer’s role and organization, or within the governance and compliance functions under the chief information officer (CIO) or chief information security officer (CISO). However, while the CIO and/or CISO often lead the development and management of protective operating controls, other functions also play critical roles in this new era.

Legal and regulatory professionals should be a core part of the regulatory assessment and advisement effort and also for the processes to achieve compliance. Most organizations begin by assembling a strong team of professionals with the right knowledge and skill sets to identify and assess gaps. This team can then design a long-term strategy that includes robust controls for monitoring and addressing change, identifying and prioritizing risks, developing more comprehensive programs, and implementing robust mechanisms to achieve internal compliance.
While it may be tempting to think of the regulatory processes at all federal agencies as being essentially the same, in practice the processes can be quite different. In particular, regulatory bodies can exhibit a wide range of statutory or precedent-based independence from the White House.

At one end of the spectrum, the Department of the Interior and the Environmental Protection Agency have been taking strong cues from the White House—developing new, potentially more flexible policies (e.g., a wide range of new measures providing support for coal), and systematically removing regulations and regulatory capabilities (e.g., eliminating a wide range of emission rules and standards). For these regulatory bodies, the current approach is expected to continue, potentially making it easier for companies to comply with the regulations that remain, and/or reducing the consequences of noncompliance.

In contrast, FERC and the CFTC now have full complements of commissioners, enabling them to conduct a more effective regulatory life cycle. Also, their technical staffs have grown more established as the turnover associated with the change in administrations has slowed down. Both of these regulatory bodies have recently shown a willingness to follow an independent approach. Case in point: While the Department of Energy attempted to draw link between coal markets and national security, FERC recently rejected the theory.

FERC has a growing focus on the overlapping issues of cybersecurity and operational integrity (including physical infrastructure and supply chain), both of which fall within its immediate mandate, and through the Standard Authorization Request (SAR) Form of NERC, on similar matters related to the BES. Similar focus and prioritization is expected to continue as well as market implications of the continued aggregation of Regional Transmission Organizations (RTO) and the impacts of renewables and alternative energy solutions on both markets and reliability.

The CFTC has had a productive 2018 as well, rewriting or clarifying specific regulations that became part of its mandate through Title VII of the Dodd-Frank Wall Street Reform and Consumer Protection (Dodd-Frank) Act. While there has been some dissent among the commissioners, the process has generally been smooth and followed the stated goals of Chairman Giancarlo.

With the CFTC’s recent leadership confirmations, there has been a responsive shift and increased surveillance and enforcement using standards for disruptive market behavior (e.g., market manipulation, spoofing, fraud). In addition, there is an increasing focus on emerging financial technology (fintech) and digital trends, such as cryptocurrency and alternative transacting platforms. These trends are expected to continue, with the CFTC investing in the development of a fintech lab environment and other innovations, as well as working proactively with industry participants and service providers. Also, while not specifically called out as a focus area, it is likely that as cryptocurrencies become more known within the broader investing community there will be an increase in related investigations and subsequent civil and criminal enforcement actions.
“Know Your Counterparty” (KYC) refers to the due diligence a company performs to help ensure it knows with whom it is dealing and can identify potential risks associated with every counterparty relationship.

Adherence to certain laws and regulations such as the Foreign Corrupt Practices Act (FCPA), the UK Bribery Act, and international trade sanctions creates the need for a strong KYC program. Although risk-based, a KYC program should be comprehensive enough to allow a company to identify and prevent money laundering, bribery, corruption, and financial fraud—and the financial and reputational risk associated with such crimes. To help ensure compliance with the laws and protect the company from being used as a conduit for committing crimes, it is recommended that all of a company’s counterparties undergo basic due diligence (at a minimum), regardless of transaction type, volume, or dollar amount.

Although KYC is most often associated with the financial services industry, nonfinancial services companies should have a strong KYC program to protect themselves—and to promote compliance with KYC-related laws and regulations. The energy industry, both in the United States and elsewhere, is coming under increasing scrutiny from regulators who are vigorously enforcing trade sanctions and anti-bribery and corruption laws. Violations of such laws carry significant financial penalties, potential criminal charges, and costly reputational damage.

Over the past two years, for example, the US Treasury Department’s Office of Foreign Assets Control (OFAC) has penalized many nonfinancial firms quite stringently. For example, a company might be penalized for entering into a contractual agreement with an OFAC-sanctioned country even if it is just agreeing to terms on projects that were already underway prior to sanctions being imposed.

The largest OFAC penalty on record for a nonfinancial institution was more than $100 million, which was imposed on a China-based telecommunications company for violating Iranian Transactions and Sanctions Regulations (ITSR). To address this issue, a company should perform a risk assessment to identify its counterparty-related risks and determine if its existing due diligence program is fit-for-purpose. It should then establish a solid infrastructure that ensures reliable data governance and ongoing monitoring of counterparty-related data. Last but not least, it should ensure adequate standards, policies, and procedures are in place that address all of the associated risks. Regulators will expect to see evidence that such measures are in place for all organizations, not just financial institutions.
On November 13, 2018, the CFTC unanimously voted to keep the de minimis threshold for swaps at its current level of $8 billion. Prior to the vote, the tentative plan had been to lower the threshold to $3 billion at the end of 2019. The possibility of this sharp reduction—and the uncertainty surrounding it—significantly hampered the energy industry’s ability to use swaps as an effective hedging tool.

The de minimis threshold was introduced in 2010 as part of the Dodd-Frank Act; however, the act made regulators responsible for setting the actual levels—triggering significant debate and questions. Businesses use swaps to hedge market risk, and placing limits on the size of their swap portfolios can significantly constrain the number, size, and duration of swaps they hold, thus limiting their ability to manage risk effectively.

For example, in the past, energy companies might have wanted to use long-term swaps to hedge the risks associated with multiyear capital investments. However, with the threat of a sharp threshold reduction looming, many companies were reluctant to commit to multiyear swaps that might make it difficult or impossible to get under the reduced threshold. This forced them to rely on a series of three- to six-month swaps instead—short-term hedges that are less effective and less appropriate for hedging long-term risk.

Now that the de minimis threshold is set at $8 billion for the foreseeable future, companies can engage in swaps with much greater certainty and confidence.

Companies can now take action on deals that might have previously been on hold due to lack of adequate hedges. Also, they now have more flexibility to develop customized swaps that can help them manage risk even more effectively than before.

It should be noted, however, that despite increased certainty about the threshold level, there continues to be some uncertainty and debate over what types of swaps will count against that threshold. The market has evolved significantly in the years since the threshold was initially established, and the CFTC is actively working to determine what definitions and methodologies make sense now and for the future regarding what should be “in” or “out” of the de minimis calculation (otherwise known as exclusions). CFTC staff welcome input from industry, which gives companies an important opportunity to shape the evolving requirements.

Now that the de minimis threshold is set at $8 billion for the foreseeable future, companies can engage in swaps with much greater certainty and confidence.
Endnotes

7. The North American Electric Reliability Corporation regulations of critical infrastructure cybersecurity are a set of requirements designed to secure assets critical to the operation of the bulk electric system or electric power “grid” (Initial Order at Mandatory Reliability Standards for Critical Infrastructure Protection, Order No. 706, 122 FERC ¶ 61,040 [2008]).
Contacts

**Leadership**

Monica O’Reilly  
Regulatory & Operations Risk Leader  
Principal  
Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
monoreilly@deloitte.com

Katie Pavlovsky  
Energy, Resources & Industrials Advisory Leader  
Principal  
Deloitte Risk and Financial Advisory  
Deloitte Financial Advisory Services LLP  
kpavlovsky@deloitte.com

Chris Spoth  
Executive Director  
Center for Regulatory Strategy, Americas  
Managing Director  
Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
cspoth@deloitte.com

**Authors**

Paul Campbell  
Principal  
Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
paulcampbell@deloitte.com

Howard Friedman  
Managing Director  
Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
hfriedman@deloitte.com

Michael Prokop  
Managing Director  
Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
mprokop@deloitte.com

The Center wishes to thank the following Deloitte professionals for their insights, contributions, and support for this report:

Chemeckia Banks, Manager, Deloitte Risk and Financial Advisory, Deloitte & Touche LLP  
Shari Gribbin, Senior Manager, Deloitte Risk and Financial Advisory, Deloitte & Touche LLP  
Joy Mayfield, Senior Manager, Deloitte Risk and Financial Advisory, Deloitte & Touche LLP  
Charlie Sanchez, Senior Manager, Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
About the Center
The Deloitte Center for Regulatory Strategy provides valuable insight to help organizations in the financial services, healthcare, life sciences, and energy industries keep abreast of emerging regulatory and compliance requirements, regulatory implementation leading practices, and other regulatory trends.

Home to a team of experienced executives, former regulators, and Deloitte professionals with extensive experience solving complex regulatory issues, the Center exists to bring relevant information and specialized perspectives to our clients through a range of media including thought leadership, research, forums, webcasts, and events.