The Outlook for Federal Compliance in the Trump Era

March 2018

Bloomberg Law

Big Law Business

Bloomberg Law

Big Law Business

About Big Law Business

Big Law Business is a Bloomberg Law website that provides news, analysis, and information about the legal profession, with a focus on the business of law. Featuring journalists from Bloomberg BNA and Bloomberg News, as well as columnists and contributors who lead and consult the world's largest law firms, corporations and law schools, Big Law Business is focused on the significant developments shaping the legal industry.

The site is designed to provide valuable information and insight to lawyers and professionals who work in big law in the United States, as well as serve as a community for discussion where thought leaders can share their views on cutting-edge trends.

About Our Special Reports

Big Law Business Special Reports are a must-read resource for all business leaders in the legal profession, including in-house counsel, law firm partners, and industry executives. These complimentary deep-dive reports are produced by Bloomberg's Big Law Business editorial team and can be downloadable as PDF files on any device.

Thank you to our sponsor for making this Special Report possible

NAVIGANT

Contents

The View on Regulation

Trump Delivers on Rollback Promises

By Dan Macy

Donald J. Trump made deregulation a pillar of his presidential campaign, and he has begun to deliver.

First came the changing of the guard in Washington. A business-friendly cabinet replaced outgoing Obama appointees, bringing with them promises—backed by the president—to scale down government involvement in corporate America.

With Trump's swearing in, a single party controlled the White House and both chambers of Congress, putting dramatic regulatory rollbacks within grasp. "We're here today for one single reason: to cut the red tape of regulation," Trump said in the White House's Roosevelt Room Dec. 14.

"We've begun the most far-reaching regulatory reform in American history," he said. "We've approved long-stalled projects like the Keystone XL and the Dakota Access pipelines. We're cutting years of wasted time and money out of the permitting process for vital infrastructure projects."

"We've begun the most far-reaching regulatory reform in American history."

Tax Reform

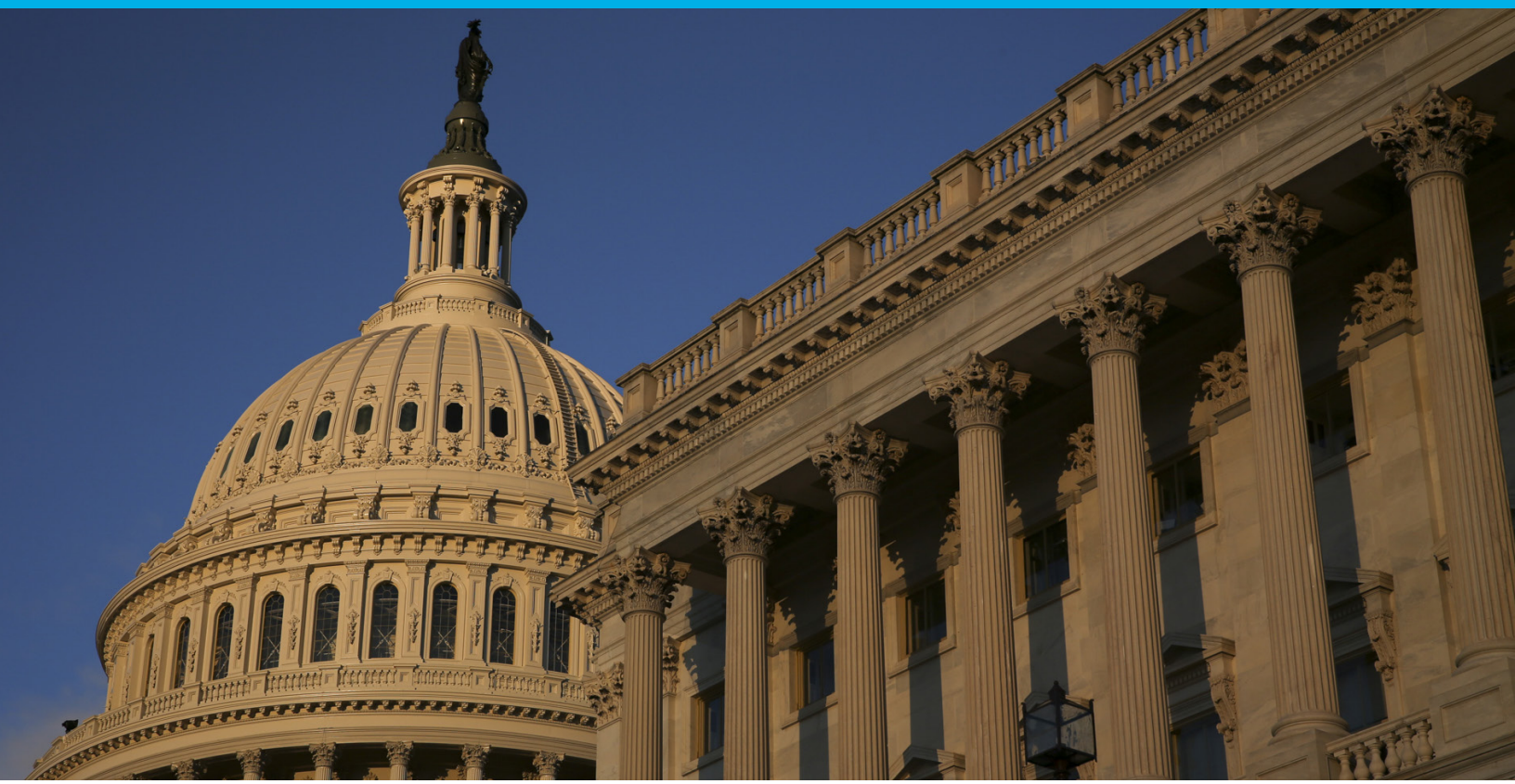
The Tax Cuts and Jobs Act became the crown jewel of the Republican Congress and Trump White House's legislative agenda when the president signed it into law Dec. 22. But the ultimate substance of tax reform is still unfolding and will be framed through a number of future actions.

The TCJA sailed through Congress in less than two months, compared to Ronald Reagan's Tax Reform Act of 1986, which required almost a year of debate. The chances are high that Congress will need to act again to clarify the details of the overhaul, or to fix drafting errors.

One of the first major unintended consequences came to light soon after passage of the tax law. Republican senators acknowledged that a drafting error gave an inadvertent tax benefit to certain agricultural businesses that buy crops. A possible legislative fix to the slipup, involving section 199A of the tax code, came in the form of a proposed spending bill resolution.

Four Republican lawmakers said in a joint statement March 13, "After discovering an unintended consequence that created an inequity within the agricultural business community, we've worked extensively with stakeholders, our colleagues, and the administration to develop a solution that will level the playing field and ensure the nation's cooperatives, independent small businesses and publicly traded firms can fairly benefit from pro-growth tax reform."

Irrespective of any future legislation, the Treasury Department and the IRS will take leading roles in shaping the revised code through regulations, reports, and guidance.



There has been immediate relief to some businesses, especially in the area of environmental regulation.

Cumbersome by Design

Outside the legislative process, there has been immediate relief to some businesses, especially in the area of environmental regulation. The Environmental Protection Agency, for example, moved in December to delay indefinitely an Obama-era ban on toxic solvents, including trichloroethylene, that had not yet gone into effect.

Since the original proposal of the ban, manufacturers may have stopped using TCE, a degreasing agent, but with the indefinite delay, companies will be ready to resume use of the chemical with minimal process change or added cost.

In March 2017, the U.S. Department of the Interior overturned a moratorium on all new coal leases on federal land, which the Obama administration had put into effect Jan. 15. The agency's action was effective immediately and directed the Bureau of Land Management to process coal lease applications and modifications "expeditiously."

Some Reversals Take Longer

But such expediencies are likely to be the exception rather than the rule, and reversing the rules will take more time.

"The public policy process is inherently incremental, which may seem like an undesirable trait, but our founding fathers designed the system to be inefficient," said Daniel F.C. Crowley, a Washington, D.C. partner at law firm K&L Gates. "Moreover, policymaking is an ongoing process, not a particular outcome. In order to achieve lasting change, there must be bipartisan agreement. Otherwise, the next administration from a different party is going to make it a top priority to undo all the policy put in place by the previous one."

A more typical example of deregulation might look more like the one that lawmakers put in the tax overhaul, seemingly to streamline employee benefit tax regulation—it is not immediately clear who would benefit or whether they would take advantage of the change, and complications lurk under the surface. Congress scrapped seven major employee fringe benefit tax breaks in the 2017 tax law, eliminating deductions for employers and income exclusions for employees.

Some changes were permanent, others temporary. Employers will now have to rethink their benefit strategies. Changes in employee benefit programs require management to perform compliance and anti-discrimination testing and announce changes to employees, as well as evaluating how a potential benefit takeaway will affect business. The loss of a tax deduction does not necessarily mean the employer will eliminate a fringe benefit.

Rolling back disclosure requirements may be what some businesses have been asking for, but with the interconnectedness of commerce, some of these rollbacks may have strings attached. Trading partners of the U.S. may take exception to any business policy considered disadvantageous to that country.

Financial Deregulation

Congress and the White House have been talking of rolling back significant parts of the Dodd-Frank Act, which aimed to address problems that surfaced during the financial crisis. The law has generally been unpopular, particularly with the finance sector, and is disliked as well by many Republican members of Congress.

But repeal of the 2,300-page law and its hundreds of regulations is simply not on the table. House Financial Services Committee Chairman Jeb Hensarling (R-Tex.) has made headway toward repealing some parts of the 2010 law. He said the Dodd-Frank Act "reaches far beyond Wall Street and does not address the real causes of the crisis," in a statement posted on his congressional webpage. In April 2017 he introduced the Financial Choice Act, which would repeal parts of the Dodd-Frank Act. It passed the House that June and moved to the Senate.

The bill enjoys industry support but is opposed by consumer groups. Paul Schott Stevens, president and chief executive of the Investment Company Institute, said in a statement at the time of the Financial CHOICE Act's introduction, "This timely bill would address flawed aspects of the Dodd-Frank Act that are not fulfilling Congress's original intent and ultimately threaten, rather than protect, investors, the financial sector, and the economy."

Around the same time, the Consumer Federation of America denounced the legislation as "a deregulatory wish list from special interests that would endanger consumers by repealing many of the significant achievements in the Dodd-Frank Act and other critical laws designed to ensure consumers, investors, and honest market participants are appropriately protected from harm in the marketplace."

The Senate on March 14 passed a bipartisan measure that would shield smaller and some mid-sized banks from some provisions of the Dodd-Frank Act, but the bill did not go as far as the Choice Act in rolling back regulations. White House press secretary Sarah Huckabee Sanders said Trump would sign the bill, which would have to be reconciled with the House first. "By tailoring regulation, the bill seeks to prevent excessive regulation from undermining the viability of local and regional banks and their ability to serve their communities," she said. The bill moved to the House, but as of press time its fate was unclear.

Whatever happens in this year's midterm elections, bipartisan agreement will be a necessary ingredient in shaping future policy. Despite Republicans' majority in both chambers of Congress, any legislation will need support from at least 60 senators to succeed.

Dan Macy is a Washington, D.C. journalist who covers regulatory affairs.

The Business of Compliance

GDPR Is Driving Record Spending

By Ellen Sheng

The EU's General Data Protection Regulation is perhaps the most wide-ranging law affecting corporate IT departments and budgets in decades. Companies, vendors, and legal firms have been gearing up to prepare for GDPR, which goes into effect May 25.

The impact on compliance budgets is considerable. According to a 2017 report by the International Association of Privacy Professionals and Ernst & Young, Fortune 500 companies will spend an estimated $7.8 billion on GDPR-related compliance and hire, on average, five full-time employees to handle compliance rules.

The $7.8 billion figure is just the start. The estimate is conservative, as "we also know that somewhere around 50 percent of companies have not addressed GDPR yet," said Trevor Hughes, president and chief executive of the IAPP. "At some point they will need to spend as well."

The consequences of noncompliance are severe.

The consequences of noncompliance are severe. Businesses face fines as high as 20 million euros or 4 percent of their global annual turnover, whichever is larger. Though privacy consultants and lawyers don't expect regulators to start imposing massive penalties straight away, "once those start to come, it will really start to hit home that [implementing GDPR] is such a big job," said Alan Rodger, senior analyst at Ovum, a London consultancy.

Wide-Ranging Changes

Companies are struggling to determine how wide-ranging the required changes can be. For example, the GDPR requirement that data not include "personally identifiable information" can encompass browser cookies, history, downloadable content, and demographic data. Though it's an EU regulation, it will have far-reaching impact on any companies that process the personal data of EU residents.

Companies vary widely in their preparedness. Not surprisingly, large global corporations are in the best shape, while smaller companies with fewer resources are less so. But even companies that have been working diligently toward GDPR compliance are finding many challenges.

"There's a gap between how companies think they manage data and how they actually manage data," said Phil Beckett, managing director at consulting firm Alvarez & Marsal.

Beckett gives a simple example: A company might have a centralized customer relationship management system that lists clients, contacts and other rudimentary personal data that's not particularly sensitive but is covered by GDPR.

With a centralized system, it's easy for companies to mistakenly believe the platform is adequately secure—that is, until they find that four or five different departments extract the information for various uses, so that it's being replicated on multiple systems across different platforms, stored on laptops, and passed around.

Beckett says compliance requires companies be able to quickly detail and document the process and respond to customer queries about personal data usage or requests that it be deleted.

American companies face additional concerns and expense because of the extra steps needed to secure data transferred out of the EU.

American companies face additional concerns and expense because of the extra steps needed to secure data transferred out of the EU. Under EU regulations, companies cannot transfer data out of the EU unless the receiving country has been deemed "adequate" under EU data protection laws.

The U.S. has not been found "adequate," as it has no broad-based privacy laws, lacks a central privacy regulator, and is viewed suspiciously because of spying by intelligence agencies, said the IAPP's Hughes.

Solutions to the problem include signing on to the privacy shield agreement or model contract provisions, but that adds an extra layer of complication for U.S. companies. "It's more than a step—it's a whole dance in and of itself that's complicated and operationally challenging," Hughes said.

Growing Industry

Hughes said he's seeing law firms struggle to take on additional GDPR engagements because of resource constraints. And the number of privacy technology vendors catering to the market also has increased dramatically. Last year, the IAPP's tech vendor report included 40 vendors. This year there are over 100, Hughes said.

GDPR is creating a big push for more compliance spending, but those outlays are expected to continue growing far beyond May 2018. Indeed, various surveys show corporate executives expect such spending to widen because of increased regulations and heightened concern about cyber risks affecting fraud, financial crime, and general business operations.

GDPR is creating a big push for more compliance spending, but those outlays are expected to continue growing far beyond May 2018.

A recent survey by Accenture found that 89 percent of compliance executives expect cost increases in their departments over the next two years. Among executives anticipating higher spending, almost half see increases of 10 to 20 percent, while about one-fifth forecast growth above 20 percent.

Another survey by Duff & Phelps, a consultancy, found compliance spending at a typical firm is expected to double in the next five years. Outlays by financial services firms is at about 4 percent of revenue, but that's expected to rise to 10 percent by 2022, according to the report.

"GDPR is a demonstration of a broader issue. We are going through a digital revolution that is creating massive issues with data protection and privacy," said the IAPP's Hughes.

"GDPR is a response to those concerns. GDPR is not our destination but rather, another waypoint in what I expect to be a long journey on this issue."

Ellen Sheng is a writer and editor with a focus on business finance, fintech, and U.S.-Asia investments.

RISK 2.0: THE DIGITAL TRANSFORMATION OF CORPORATE COMPLIANCE

By: Navigant Disputes, Forensics, and Legal Technology Experts

In the information age, where industries must "go digital" or be left behind, corporate compliance officers must undergo technological transformations as their companies look to them to face increasing cyber threats and regulation.

Going forward, technology will affect compliance operations by:

- **Exposing companies to risk through employee emails, financial data, cloud applications, electronic records, mobile devices, wearables, and social media.**
- **Improving compliance through platforms including regulatory technology (RegTech), artificial intelligence (AI), blockchain, automated risk assessment, and data loss prevention software.**

Technology Threats

Compliance officers typically oversee business ethics and compliance, uphold regulations, and manage risk. However, as technological capabilities increase, they must also address cybersecurity concerns.

Email, the most common workplace technology, also provides easy access to computer networks. Simply by opening inconspicuous attachments, employees can trigger malware attacks.

Mobile devices and wearables are also potential portals for cyber criminals. Hackers can penetrate business emails or company files through employees' personal accounts.

Employees should think twice before tweeting on company devices – social media can facilitate security breaches, as can web-based collaboration tools including Box, SharePoint, Yammer, and Google Hangouts.

In the healthcare industry, hackers target hospitals, clinics, and physicians to access patients' personal identification and health information, enabling them to drain bank accounts and run up credit card charges.

Along with these growing cyber threats, compliance officers must navigate a vast regulatory landscape.

For example, the new European General Data Protection Regulation (GDPR) outlines the collection and use of personal information on the internet, and recent New York State Department of Financial Services regulations protect financial services companies from cybersecurity threats. Meanwhile, the healthcare field faces constant regulatory updates surrounding electronic medical records, patient privacy, and performance outcomes.

NAVIGANT

Learn more at Navigant.com/legal

Technology Solutions

Fortunately for compliance officers, technological tools help address these cyber threats and the resulting regulatory maze.

RegTech software helps financial services companies track and comply with regulations through consistent interpretation and analytical identification of suspicious activity.

Emerging AI technology uses machine learning programs to adapt over time. By completing tasks, AI learns about relevant subjects and produces increasingly accurate results.

Blockchain activities, popular in bitcoin transactions, are encrypted and immutable. Once enacted, transactions are documented and unalterable, virtually eliminating fraud.

Automated risk assessment technology probes organizational data, identifies potential vulnerabilities, and develops action plans to repair breaches.

Data loss prevention software locates corporate data on networks, the cloud, mobile devices, and other sources; tracks how it is used; and protects information from being compromised.

Governance, risk, and compliance (GRC) technology aligns, leverages, and automates processes. GRC centralizes risk reporting while providing a holistic view of risk and compliance coverage and exposures.

New Opportunities

Understanding technological threats and protection strategies may seem like one more demand placed on compliance officers. However, staying informed is critical in reducing risk, and may mean the difference between a massive security breach and a successful defense of a cyber attack.

By incorporating sound governance and protection system technologies, and identifying potential vulnerabilities, compliance officers can help their companies achieve and maintain success.

Technologies Compliance Officers Should Know

Wearable Sensors Raise Workplace Privacy Concerns

By Ellen Sheng

As the territory occupied by wearables is pretty much uncharted, there are few constraints.

The growing industry that supplies wearable and connected devices like cameras, work tags with sensors, and GPS and health trackers, which are increasingly seen in the workplace, is facing a plethora of compliance questions.

By some estimates, about 15 percent of Fortune 500 companies are now using sensors, ID badges, and other technology to collect data about employees. Companies and employees alike are uncertain just how to view the devices, whether they're worthwhile, and if they should accept them.

"It's the Wild West right now," said Jeff Pollard, principal analyst on security and risk at Forrester Research. "Technology is innovating at such a rapid pace, often governments are passing regulations or adopting regulations that solve problems from two to three years ago."

And as the territory occupied by wearables is pretty much uncharted, there are few constraints on companies using the technology in any way they wish.

"Very little U.S. privacy law actually applies to data. It actually applies to particular entities who are regulated as holders of the data," said Lee Tien, senior staff attorney at the Electronic Frontier Foundation. Though some states may have laws on the books, there's nothing that's particularly effective, he said.

"Within the workplace, virtually any law that protects your rights can allow you to waive those rights. Even if someone said 'no, you can't use mood-sensing tech,' they can be easily forced to agree," Tien said. That is, unless a new law states that companies can't make workers say they agree to the technology.

Uncertain Benefits

One characteristic of wearables and sensors is the sheer amount of data they can collect. An industry of providers is creating all kinds of affordably priced sensors and marketing them as a means to enhance employee performance or lower energy bills.

Companies can use sensors placed inside ID badges that can track productivity by monitoring employees' tone of voice, posture, and location within the office. Firms such as UPS use GPS to track vehicles and packages and can also locate employees. Cameras and sensors can measure workplace environmental conditions—potentially saving on heating and cooling bills or flagging dangerous chemical exposure.

Corporate wellness programs are distributing health trackers such as Fitbits. In professional sports, leagues have started using biometric devices to track heart rate, skin temperature, sleep cycle, and other factors.

But though the technology is there, the rules governing the use of these devices are not. There are legitimate concerns about how this data could put pressure on employees or affect compensation. The lack of regulation and precedent create an uncertain environment where anything goes.

"Generally with surveillance in the workplace, there is no federal law protecting workers from being tracked or surveilled," Tien said.

Forrester's Pollard has doubts about the benefits of using sensors and wearables.

"There are so many other things companies can do to optimize performance. It would take an incredibly well-run business before [wearables and sensors] become the optimization to go to." The hazy legal environment could also mean that companies implementing some form of sensor technology might find themselves in legal hot water several years down the road.

Beside questions of privacy and regulation, wearables also open the door to potential security breaches.

"One of the rules of security is that if you have physical access to the device or wearable, then security is out the window. If they can touch it, they can hack it," Pollard said. The growing number of devices with potentially sensitive information on them "extends a company's attack surface," he said.

Any device that collects information and shares it by mobile or other means can be breached. Moreover, most wearables are controlled with an app or web-based interface that can also be hacked.

Best Practices for Early Adopters

Some early adopters are grappling with privacy issues and finding solutions. For instance, the NBA last year signed an agreement with the National Basketball Players Association under which players have the right to know what is being tracked, have rights to the data, can stop wearing the device at any time, and are assured the data won't be used in contract negotiations.

UPS drivers recently negotiated a contract that precludes the company from imposing disciplinary measures using only data collected from GPS tracking.

From a best practice standpoint, "think what kind of workplace you want and what kind of workers you want," Tien said. "There's a lot of monitoring in the workplace that people will accept if you are honest with them about why it's important."

Consultants also advise companies to look carefully into the data being collected by the devices. What kind of data is it, why is it being collected, and where does it go? How is the data being used? There is a good chance that companies selling data-gathering devices also sell the collected data.

Tien said it's a good idea for companies considering worker surveillance technology to form an internal policy group that includes worker representatives and management to get a sense of how the workforce feels about it.

"Fundamentally, the kinds of technology used to track people can be dehumanizing, so it's good to avoid that risk by being humane and talking to people about the issue," Tien said.

"There's a very thin line between new and creepy," said Forrester's Pollard, "and technology crosses that line often."

Wearables also open the door to potential security breaches.

Ellen Sheng is a writer and editor with a focus on business finance, fintech, and U.S.-Asia investments.

Reduce your risk.
Protect your organization.

Compliance-focused expertise and tools that get you the answers you need – quickly.

Advise on a wide range of regulatory and compliance issues.

Provide strategic advice.

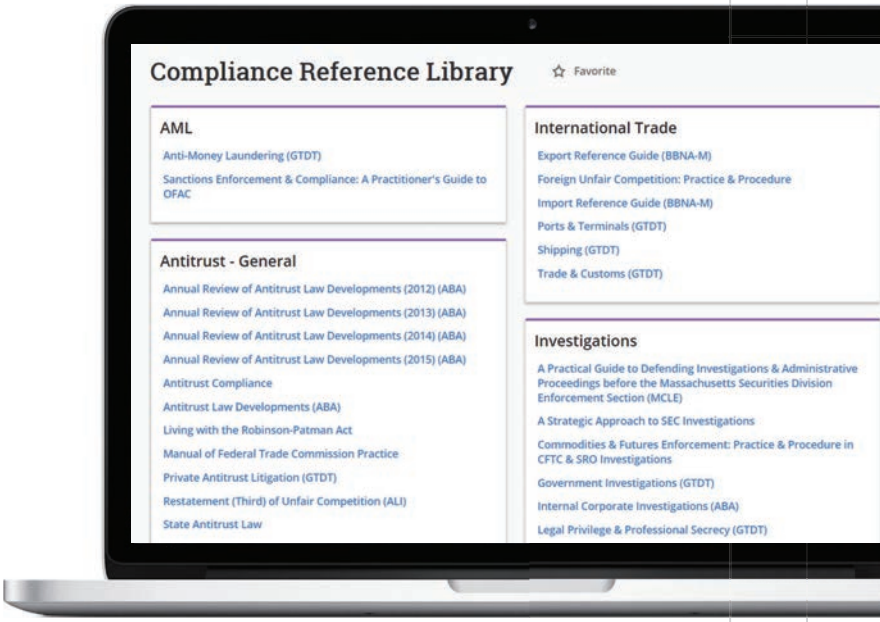
Proactively identify and mitigate risk.

Bloomberg Law® is your key. Access the news, analysis, and timesaving practice tools you need to stay in compliance and avoid costly missteps – today and tomorrow.

The future is here.

Define it with us.

bna.com/bloomberglaw



Bloomberg Law®

Changes in the Public Contracting Arena

2018 NDAA Will Affect GAO Bid Protests

By Milton C. Johns, Esq.

President Donald Trump's signing of the fiscal year 2018 National Defense Authorization Act in December 2017 put in motion several changes to the federal procurement bid protest system.

The 2018 NDAA requires the Department of Defense to implement a "loser pays" pilot program for bid protests.

One change that could significantly impact the government contracting industry is adoption of a pilot program requiring protesters who unsuccessfully challenge Department of Defense contract awards to pay the costs of those protests.

Under the Competition in Contracting Act, disappointed bidders may, under certain circumstances, protest the award to the successful bidder at the Government Accountability Office. The protest must allege a flaw in the process that violated federal procurement law, such as failure by the contracting officer to follow the terms of the solicitation under which the procurement was made.

It's possible for a contracting officer to make a bad choice if he or she follows a fair process for the selection, so the tribunal deciding a protest will not second-guess or replace the contracting officer's judgment with its own.

The most prevalent reasons for sustaining protests during fiscal year 2017 were unreasonable technical evaluation, unreasonable past performance evaluation, unreasonable cost or price evaluation, inadequate documentation of the record, and flawed selection decision.

"The financial incentive that large contractors have to protest, to earn profits during the 100-day period, will not exist or may be reduced."

Filing a protest with the GAO also triggers a 100-day stay of the contract award, during which GAO must render its decision. Some industry and federal procurement officials have complained that the stay of up to 100 days can hamstring efficient operation of the government, particularly in matters involving national defense and homeland security. Others complain that because there are no consequences for an unsuccessful protest, there is almost no reason not to protest an unsuccessful award.

Responding to government and industry concerns, the 2018 NDAA requires the Department of Defense to implement a "loser pays" pilot program for bid protests. Under the pilot, if a disappointed bidder with annual revenues in excess of $250 million protests a Department of Defense contract award, and that protest is denied by GAO, then the contractor must reimburse the Department of Defense for costs incurred in responding to the protest.

The pilot program will run for three years and will cover protests filed between Oct. 1, 2019, and Sept. 30, 2022. At the conclusion, the Department

of Defense will need to determine the effectiveness of the "loser pays" regime and report to the House and Senate Armed Services Committees on whether to make the pilot permanent.

David Yang, government contracts partner at Blank Rome law firm, sees the potential results from the pilot program as a "mixed bag." Because the "loser pays" provisions apply only to bidders with annual revenues in excess of $250 million, "the procurements subject to protest are typically larger, usually involve a larger record/more issues, and are generally more expensive to litigate."

He said protesters will be deterred from filing "if the protester is not an incumbent; or if the protester is an incumbent, the procurement is of a smaller dollar amount."

"The financial incentive that large contractors have to protest, to earn profits during the 100-day period, will not exist or may be reduced," Yang said. "But, for incumbents, if the profits expected during the stay are sufficient to mitigate their exposure to potential cost shifting, I think they will still protest."

In the GAO's November 2017 report to Congress on bid protests, the total number of bid protests filed was down 7 percent from fiscal year 2016. This decrease ended a four-year upward trend in the number of bid protests filed at GAO.

While only 17 percent of bid protests were successful on the merits in fiscal year 2017, meaning the GAO agreed with the protester and sustained the protest, nearly half—47 percent—of protesters did receive some relief from GAO because of the bid protest.

The details of the pilot program are yet to be established, and the Department of Defense will have two years from the date of the president's signature to implement the program. Large government contracting firms nonetheless will need to reevaluate their bid protest strategies with the prospect of having to fund the costs of their failed protests beginning in fiscal year 2020.

Smaller businesses will be reassured that the pilot program will not affect their ability to protest without the chilling prospect of bearing the cost of an unsuccessful action. The move does, however, signal Congress's willingness to explore alternatives to improve and streamline the federal acquisition and procurement system.

Milton C. Johns is partner and Government Contracts Practice chair at FH+H PLLC.

Regulatory Shifts in Finance

2018 Outlook

By N. Peter Rasmussen

The past year promised dramatic changes in financial regulation. A new president, one-party control of Congress, and a new cast of regulators seemed to indicate a profound shift was imminent. Congress jumped in, only to retreat with little to show for its efforts. The Securities and Exchange Commission, under new Chairman Jay Clayton, has proposed modest changes and is looking this year to streamline regulations to encourage more issuers to register as public companies.

Congressional Activity

President Donald Trump came into office promising to "do a big number on Dodd-Frank," the landmark legislation passed in 2010. The House of Representatives acted, passing the Financial Choice Act, crafted by Rep. Jeb Hensarling, chairman of the House Financial Services Committee in June 2017. The bill, which would have repealed or weakened many Dodd-Frank Act provisions, then stalled in the Senate.

Congress overruled some Consumer Financial Protection Bureau and SEC regulatory measures and passed parts of the Choice Act, but appeared to lose interest after turning its attention to health care and tax legislation.

Now Congress has returned to financial regulation. The Economic Growth, Regulatory Relief, and Consumer Protection Act, sponsored by Sen. Mike Crapo (R-Idaho), has a good chance of becoming law.

The assumption underlying the bipartisan bill, which passed the Senate on March 14, is that Dodd-Frank hurt local and regional banks. The selling point for Democratic supporters is that the largest Wall Street banks are excluded from one of the Crapo bill's major benefits. The legislation raises the threshold for treatment as a "systemically important financial institution" from $50 billion in total consolidated assets to $250 billion.

Under Dodd-Frank, a bank in that category must comply with enhanced regulation, including higher capital requirements and regular stress tests. For banks, stress tests—which use hypothetical situations to assess an institution's ability to withstand various threats—can be extremely costly.

Opponents argue the bill goes far beyond easing regulatory burdens on credit unions and neighborhood banks, as some of the largest institutions would be exempt from enhanced oversight. While the biggest banks would remain subject to stress testing, Countrywide Financial, one of the largest institutions to collapse during the financial crisis, would not have been under the Crapo bill.

In its first floor vote, the bill garnered 67 votes. If it passes the Senate, the two chambers will try to reconcile drastically different proposals. The House version effectively repeals Dodd-Frank, while the Senate bill leaves much of the law intact. Given the split in their caucus over the far less expansive Senate version, it is doubtful Senate Democrats would concede much in further Dodd-Frank rollbacks.

Regulatory Agency Approaches

The financial industry may be more successful in getting changes from regulators than from Congress. Under Trump appointees, agencies such as the CFPB and Office of the Comptroller of the Currency may relax regulations such as the Volcker Rule, which prohibits banks from trading with their own funds, and limits loans characterized as predatory.

Perhaps the most significant proposal involves disclosure provisions in Regulation S-K. Mandated in the 2015 Fast Act, it calls for removing outdated disclosure requirements and simplifying reporting on properties owned by registrants. Companies could exclude personal information from filings and eliminate repetitive reporting in the Management's Discussion and Analysis portion of annual reports.

The commission will also consider eliminating outdated and redundant provisions in agency accounting rules under Regulation S-X. And the Division of Corporation Finance is considering recommending amendments to Regulation S-X that affect disclosure of financial information of acquired businesses.

There are other areas to watch. Clayton has endorsed expanding the number of issuers registered with the agency as public companies, as well as easing the regulatory burden on public companies. Last July, the agency's Division of Corporation Finance expanded the availability of confidential submission of draft registration statements, previously open only to smaller "emerging growth companies," to all issuers.

Clayton staked out two priorities in enforcement. The first involves protection of retail investors, including development of a Retail Strategy Task Force. For example, the SEC last month announced a self-reporting initiative to protect advisory clients from undisclosed conflicts of interest and to return money to investors in cases in which an adviser selects a more expensive mutual fund share class when a less expensive one for the same fund is available and appropriate.

The SEC will also focus on blockchain and digital currencies. Clayton stated that many digital tokens sold in initial coin offerings may be securities, making their sellers subject to federal securities laws. He also expressed concern with the lack of transparency in the offerings.

Similarly, the SEC's Office of Compliance Inspections and Examinations, which oversees broker-dealers, investment companies, and investment advisers, announced last month that it will concentrate on cryptocurrencies and ICOs. Areas of focus include whether financial professionals maintain adequate controls to protect these assets from theft or misappropriation, and whether they provide investors with disclosure about the risks associated with these investments—including fraud.

N. Peter Rasmussen is a senior legal editor with Bloomberg Law, concentrating on corporate transactions and federal securities law.

Bloomberg Law

Big Law Business