MOFO
GLOBAL PROCUREMENT QUARTERLY

Spring 2015

IN THIS ISSUE

RIGHT TO MODIFY?

When can an existing public contract be amended without undergoing a new procurement process?

By Alistair Maughan and Sarah Wells

Across Europe, public bodies are under increasing pressure to streamline their services and ensure that their relationships with suppliers continue to deliver value for money. It is therefore common for a public body to seek to amend its existing contract to meet evolving requirements. But the EU procurement rules impose limits on the legitimacy of contract amendments, and that presents risks for both authorities and contractors.

Under the EU procurement regime, if amendments to an existing public contract are too extensive, the public body may find itself in breach of the public procurement regime – with the result that the amendment is susceptible to the risk of legal challenge.

A key 2008 European Court of Justice (CJEU) case from Austria established the principles and constraints within which authorities must work. And the updated EU legislation on which we reported in the Winter 2015 edition of the Global Procurement Quarterly codified the prior case law. Recently, a case in the UK has served as a reminder of the issues that public bodies and their contractors must consider if they wish to amend their existing contracts.

Gottlieb v. Winchester City Council

In 2004, Winchester City Council (WCC), entered into a development agreement for the redevelopment of the Silver Hill area of the city of Winchester, UK. In June 2014, the developer approached WCC to seek approval for amendments to the development agreement in accordance with its terms.

These amendments included removing the requirement for a bus station, removing the requirement for a market store, amending a provision in respect of affordable housing by substituting a financial contribution based on future viability of the scheme (up to the equivalent of 40 percent affordable housing), and increasing the rent payable by the developer as a result of increased retail space. The amendments were agreed to by WCC in August 2014. Mr. Gottlieb subsequently applied for a judicial review of WCC's decision to authorize these amendments, arguing that the amendments were materially different in character from the original contract to such an extent as to be tantamount to a renegotiation. Therefore, the amendments should be held to be unlawful because no new procurement exercise had been carried out.

When is an amendment a material amendment?

The court ultimately had to decide whether the amendments to the development agreement were so substantial as to require a new procurement procedure. Notably, this case was heard before the Public Contracts Regulations 2015 (2015 Regulations) came into force in England and Wales.[1] Therefore, the decision had to be made based on existing case law – in particular, the CJEU decision in *Pressetext Nachrichtenagentur GmbH v. Republik Osterreich*.

The CJEU in *Pressetext* stated that amendments are material where they are "materially different in character from the original contract and, therefore, such as to demonstrate the intention of the parties to renegotiate the essential terms of that contract." This would include amendments:

- That introduce conditions which, had they been part of the initial award procedure, would have allowed for other tenderers to be admitted or for a different tenderer's bid to have been accepted;
- That extend the scope of services to those which were not originally covered; or
- That tip the economic balance in favor of the contractor in a manner not provided for in the terms of the initial contract.

With regard to other bidders, the court held that evidence of actual or potential bidders may assist, but was not required in assessing these facts. It can be sufficient to demonstrate that a "realistic hypothetical bidder" would have applied if the contract had been advertised.

Was the development agreement materially amended?

WCC argued that the amendments were made to the development agreement because the project was not viable on the original terms and, therefore, would not have been able to proceed had the amendments not been made.

In assessing whether the amendments were material, the court had to look at each of the amendments made to the development agreement. For each amendment, the court held that:

- Removing the requirement for a bus station meant the developer no longer had to pay for it and also would have increased profit making retail space. This change was not anticipated in the contract and a potential bidder could not have anticipated this change. Therefore, applying *Pressetext*, the court found that this was a material change to the contract because the economic value should be judged by potential profits to be obtained from third parties and not just from the value of the contract.
- Amending the affordable housing requirement to permit replacement of affordable housing with an off-site sum towards affordable housing with a claw-back mechanism based on future profits was a material change because it would have made the contract significantly more valuable to bidders.
- Extending the long stop date such that, instead of being able to terminate the contract within five years if specified conditions had not been discharged (or waived), an agreement was reached not to terminate prior to June 2015, benefited the developer by providing additional time for development and more time to recover its upfront costs.

The variation clause

Although a variation clause was included in the WCC contract, because the amendments made to the development agreement related to issues that played a "decisive factor" in the award of the contract, a fresh procurement process was still required. In addition, any variation clause should be specific and the invitation to tender should set out the relevant rules to maintain equality and inform potential tenderers that variation is a possibility.

In this case, WCC had absolute discretion on whether to grant approval under the variation clause. The court held that the variation clause was so broad and generic that it did not meet the transparency requirement.

The decision

The court held that there was evidence that other potential bidders, with a realistic prospect of success, would have bid for the contract. This was due to (i) the terms being more favorable following the amendments; (ii) Winchester being a place of desirable commercial opportunity and therefore attractive to other bidders; and (iii) other companies being in a position to have been able to bid. Thus, Mr. Gottlieb's challenge succeeded and the proposed amendment had to be unwound. The original contract remained in place without the proposed changes.

The 2015 Regulations

As noted above, the 2015 Regulations came into force in the UK in February 2015. The 2015 Regulations clarify when contracts can be modified without undergoing a new procurement process. Regulation 72 sets out specific circumstances in which a new procurement procedure is not required as a result of contract modifications, including:

- Where any modifications, irrespective of their monetary value, have been provided for in the initial procurement documents in clear, precise, and unequivocal review clauses; price revision clauses or options may be included, provided that these state the scope and nature of possible modifications or options, as well as the conditions under which they may be used and do not provide for modifications or options that would alter the overall nature of the contract;
- For necessary additional works (services or supplies) where a change of contractor cannot be made for economic or technical reasons (e.g. interoperability), or because such a change would cause significant inconvenience or substantial duplication of costs for the contracting authority; this is, however, subject to an increase in price not being above 50 percent of the value of the original contract;
- Where the need for modification has been brought about by unforeseen circumstances and (i) the required modifications do not alter the overall nature of the contract; and (ii) any increase in price is not above 50 percent of the value of the original contract; and
- Where the modifications, irrespective of their value are not substantial (e.g., the modification does not render the contract materially different in character from the one initially concluded, the modification does not extend the scope of the contract considerably, or a new contractor replaces the one to which the contracting authority had awarded the contract (unless such change is as a result of (i) an unequivocal review clause or option or (ii) a universal or partial succession into the position of the initial contractor by merger/takeover/restructuring, etc., where such new contractor fulfils the original selection criteria, if such switch is not designed to circumvent the procurement rules and no other substantial modifications to the contract occur)).

Many of the factors set out in Regulation 72 effectively codify the principles set forth in *Gottlieb v. WCC*. Furthermore, under Regulation 73, contracts will be deemed to include a right of termination upon the occurrence of certain events, one of which includes material changes to the contractual terms. Thus, the 2015 Regulations should give more clarity to all parties concerned because a new procurement procedure must be followed for contract amendments unless the modifications meet the Regulation 72 requirements.

1 As previously reported in the Procurement Quarterly Winter 2015 edition, the 2015 Regulations implemented, within the UK, a number of EU-level changes to the procurement regime including simplifying the procedures to make the regime more flexible and widening access for SMEs.

INTERNATIONAL BRANDS MAY TRIGGER CROSS-BORDER INTEREST IN EU TENDERS

The European Court of Justice extends applicability of general EU procurement principles to so-called "below-threshold contracts" in international brand case.

By Felix Helmstädter and Philipp Westerhoff

The Court of Justice of the European Union (CJEU) has recently clarified the procurement rules that apply to low value contract awards – and, in doing so, has raised the prospect that referencing an international brand in the technical specifications may trigger greater compliance requirements.

Introduction

It is generally known that, in the European Union (EU), the strict rules on public procurement, as prescribed by

the harmonized framework of the EU Public Procurement Directives (PPD), apply when contracting authorities purchase goods or services for a price that exceeds certain financial threshold values. For public service and supply contracts, the current thresholds are set at €207,000 for local authorities and €134,000 for central government departments and agencies respectively. For public works contracts the current threshold is €5,186,000.

However, so-called "below-threshold" (*i.e.*, low value) contracts are a key economic factor within the EU. Around 82 percent of the total annual amount of EU-wide public expenditures, approximately €2,400 billion, involve low-value contracts. Thus, below-threshold contracts may still represent major opportunities for businesses operating in the EU.

Nevertheless, depending on the relevant legislation in each Member State and the estimated value of the contract concerned, often no (or only rather vague) national rules apply to the awarding of such contracts. As a consequence, tender procedures are more often affected by the arbitrary practices on the part of the contracting authority or contracts are directly awarded without any competitive tendering.

Cross-Border Interest

In a recent decision, issued on April 16, 2015 (case C-278/14), the CJEU reaffirmed the importance of low-value EU contracts. The court emphasized that, where a contract has a "cross-border interest" (*i.e.*, an economic interest for companies located in other Member States), it must still be awarded in compliance with the EU's general principles of equal treatment, non-discrimination, and transparency, as articulated in the Treaty on the Functioning of the European Union.

In this regard, the decision is in line with prior CJEU rulings. According to the established EU case law, a cross-border interest may exist if, for example, the value of the contract only marginally falls short of meeting the thresholds, or there is a geographical nexus between the location where the contract has to be performed and an adjacent Member State.

The Impact of an International Brand Reference

In its recent decision, however, the court seems to extend the field of application of the general EU principles to contracts well below the relevant thresholds if certain other criteria are implicated.

The CJEU was asked by a Romanian court to respond to specific questions about a tender for a contract to supply computing systems and equipment valued at €58,000 (the threshold for supply contracts was €200,000 at that time).

In the tender documents, the contracting authority referenced a specific brand of microprocessor ("Intel Core i5 3.2 GHz or equivalent") as part of its technical specification and all bidders were required to offer a product that at least corresponded to the referenced processor.

The contracting authority rejected an offer that included a processor that fully complied with the requirements initially set forth by the authority. At the time it rejected the offer, the authority changed the technical specification, rationalizing that the manufacturer had stopped production of the referenced processor and substituted a next generation processor. The authority used the modified technical specification to disqualify the tenderer.

The court stated that the national court must assess whether the general EU principles are applicable in cases involving low-value contracts by analyzing whether a cross-border interest exists in the particular case. Nevertheless, despite the instruction to the national court, the CJEU suggested that, although the contract at issue had a value of less than €60,000, it could still trigger a cross-border interest because the "*case concerns the supply of computing systems and equipment with the reference processor being that of an international brand.*"

Having indicated that a cross-border interest may be triggered by the reference to an internationally branded product, the CJEU applied the general EU principles to the case. The CJEU held that the contracting authority should be prohibited from rejecting the tender because there was no justifiable basis for modifying the original technical requirements. In particular, in the court's view, it is irrelevant whether or not the referenced product is still in production or available on the market. According to the court, the contracting authority is bound by, and cannot arbitrarily disregard, the conditions it imposed in the tender.

Procedural Minimum Standards for Below-Threshold Procurement

According to the CJEU decisions and corresponding EU Commission guidelines, once a cross-border interest is implicated, a contracting authority has to comply with a set of procedural minimum standards including:

- Adequate advertising for the benefit of any potential tenderer;

- Clear description of the subject matter of the contract;
- Equal access for economic operators from all Member States;
- Mutual recognition of qualifications;
- Appropriate time limits;
- Non-discriminatory contract award decision; and
- Judicial protection.

Conclusion

The CJEU has equipped tenderers with additional arguments to force contract authorities to comply with procedural minimum standards even where a specific contract fails (by far) to meet the EU financial threshold values. In particular, it could be argued that a cross-border interest exists when a contract authority either references an internationally branded product in its technical specifications or whenever technical standards are defined, *de facto*, by global market players. The judgement also serves as a reminder, to contract authorities, to abstain from arbitrarily amending technical specifications or other tender conditions once a public tender has been advertised.

INTERVIEW WITH FORMER SENIOR DOJ WHITE-COLLAR PROSECUTOR, JAMES KOUKIOS

James Koukios has joined the firm's Litigation Department as a partner in the Securities Litigation, Enforcement & White-Collar Criminal Defense practice resident in the Washington, D.C. office. Mr. Koukios is the second high-ranking DOJ prosecutor to join MoFo in the past year, following the 2014 arrival of former Fraud Section Deputy Chief Charles Duross. In his most recent position, Mr. Koukios oversaw the Foreign Corrupt Practices Act, Health Care Fraud, and Securities and Financial Fraud Units. With the addition of Mr. Koukios, who previously served as an Assistant Chief in the FCPA Unit, MoFo is the only law firm in the world with two former FCPA Unit managers. During his tenure at DOJ, Mr. Koukios worked with domestic and foreign law enforcement authorities around the globe. He tried nearly two dozen jury cases, serving as a lead trial attorney in two landmark FCPA-enforcement trials: *United States v. Esquenazi* and *United States v. Duperval*. In addition to his service to DOJ, Mr. Koukios served as Special Counsel to the FBI Director, advising the Bureau's leadership on criminal enforcement policy, congressional testimony, and interagency issues.

What attracted you to Morrison & Foerster?

The firm's global platform, deep bench of talented attorneys, extensive roster of technology and life sciences clients, and its reputation for collegiality were among the many factors that attracted me to the firm. I look forward to continuing the firm's success in helping clients navigate complex white-collar matters including cross-border anti-corruption challenges.

What do you consider some of the highlights of your tenure at DOJ?

Serving my country as a federal prosecutor for over a decade was, in and of itself, a highlight. As far as specific highlights, the *Esquenazi* and *Duperval* trials rank right up there. Both came at a time when DOJ's ability to win an FCPA case at trial was being heavily questioned. But we were confident in our facts and our legal theories, and the jury, trial judge, and, ultimately, the Court of Appeals agreed. Another highlight that spanned my time in Miami and the Fraud Section was the AEY case, which involved a $298 million defense contract to supply ammunition to the Afghan National Army and Police. While we were investigating potential fraud and export licensing violations, a really terrific reporter from *The New York Times*, CJ Chivers, also started investigating the case and ended up publishing a front page, top of the fold piece in the Sunday *NY Times*. We ended up successfully prosecuting the company, three executives, and a financier for defense procurement fraud and made new law along the way.

From your experience overseeing the Health Care Fraud Unit, what are the important lessons for companies based on recent enforcement activities?

Health care will continue to be at the center of federal criminal and civil law enforcement, including through the False Claims Act, for years to come. The aging population and expanded coverage through the Affordable Care Act are factors that will serve to maintain and increase this trend. The Fraud Section's move back into corporate health care fraud enforcement is also potentially significant. By leveraging the Health Care Fraud

Unit's deep expertise in prosecuting individuals and the Section's overall expertise in corporate prosecutions, the corporate health care fraud initiative, which I was fortunate to be a part of as Senior Deputy Chief, has the potential to make the Fraud Section a significant player in this arena, joining DOJ's Civil Division and several prominent U.S. Attorney's Offices.

In addition to the increase in the number of people eligible for federal health care programs, what other trends are causing the increase in cases involving the False Claims Act?

One additional factor (perhaps the most important factor) is economics: FCA cases present the opportunity for *qui tam* plaintiffs, and their lawyers, to recover a substantial portion of any ultimate award, which, by design, encourages more *qui tam* filings. The more *qui tam* cases filed, the more likely it is that the government will be made aware of potential problems with certain claims and initiate its own investigation. FCA cases have also proven to be lucrative for the government, as evidenced by DOJ's settlement statements, which routinely tout the record recoveries for tax payers. Indeed, in November 2014, the Acting Associate Attorney General and the Acting Assistant Attorney General for the Civil Division trumpeted the fact that the Department had achieved the three largest annual recoveries ever recorded under the FCA in the last three years, including in 2014, when recoveries topped $5 billion for the first time.[1] With these demonstrated financial incentives for both the private plaintiffs' bar and the government, we can expect this trend to continue.

What should companies be aware of to help ensure they do not become the target of an FCA investigation?

First and foremost, compliance. Companies must implement robust compliance programs that are appropriately tailored to their businesses, the applicable laws and regulations, and their particular government contracts—and they must then ensure that the compliance programs are effective. One particularly good way to do this is to involve internal audit in the compliance process. Internal audit may detect potential problems before the government is ever involved and may catch problems before they balloon into a major problem. The low intent threshold under the FCA makes it particularly important that even inadvertent mistakes be detected and remediated early on. Moreover, the government is often impressed by the involvement of internal audit in a compliance program because it demonstrates that a company's compliance program is not just a "paper program" but is instead being implemented earnestly and that any systemic problems identified by internal audit are fixed or revised appropriately. This can increase the chances of a more positive outcome for a company if the government does get involved.

Lastly, to the extent possible, it is good to create and maintain an open dialogue with the contracting officer. The meaning and applicability of regulations or particular contractual provisions are not always clear. If doubts arise about certain requirements, it is important to have a good relationship with the contracting officer to discuss the unclear issues and the company's expected path forward. This type of dialogue can help prevent problems altogether and, if problems arise, may help form the basis for a defense that the government was given notice that the company was taking particular actions based on its understanding of the requirements.

Why should companies self-report potential issues under the FCA?

Depending on the circumstances, a company may be required to timely self-disclose credible evidence of certain violations of the FCA. Where disclosure is not required, the decision to self-report issues (FCA or otherwise) to the government is a difficult one and may not always be correct. However, there are some potential benefits to consider when weighing the options. First, a self-disclosure may help reduce the amount a company has to pay by lowering damages or avoiding penalties. Second, self-reporting may help build credibility with the government by demonstrating that the company has an understanding of, and a handle on, its operations and intends to promote compliance with applicable laws and regulations. This can have several potential benefits, such as reducing the likelihood that the case will be brought criminally, that a corporate integrity agreement will be imposed, or that the company will be suspended or debarred, all of which can have a much more dramatic and long-term impact than an adverse monetary judgement. Regardless of whether a company ultimately chooses to self-report, it is critical that the company thoroughly investigate—and remediate—any problems. The worst thing a company can do is to ignore a problem.

If you had to identify the biggest areas of anti-corruption concern for companies and their executives, what issues stand out?

Over the last several years, we've seen that no industry is immune to FCPA risk. For example, where the extractive, energy, defense, health care, and technology industries have long been at the center of FCPA enforcement, we have recently seen significant investigations in the retail and financial service industries. For example, the individual prosecutions in the Direct Access Partners case, in which I was personally involved, illustrated that, in addition to anti-money laundering and regulatory risks, those working in the financial services industries can also face FCPA risks when dealing with foreign officials.

In terms of specific risk areas, third-party intermediaries continue to be the most significant risk for many companies. From the moment I arrived at the Fraud Section's FCPA Unit in 2009, I was struck by how many investigations involved the laundering of bribes through payments to consultants and other third parties. As amply demonstrated by the record-setting Alstom resolution, which I oversaw, this risk hasn't lessened over the years. What this means for companies and their executives is that the compliance and audit functions have to be fully empowered and resourced, and the company's internal controls have to be robust, well designed, and faithfully deployed to prevent, detect, and remediate violations involving third parties.

Are non-U.S. governments stepping up their anti-corruption enforcement activity?

Absolutely. From the UK to Brazil to Indonesia, and in between, non-U.S. governments have stepped up their anti-corruption enforcement activities in recent years. Through international organizations such as the OECD and other, more informal means, enforcement authorities from many countries are establishing relationships, sharing best practices, and sharing information as never before. China's recent activities in this space are also potentially game changing. What all this means is that it is more likely than ever before that corrupt activities will be detected, investigated, and prosecuted and not always by the U.S. alone.

What are your predictions for the coming year regarding priorities for securities and financial fraud enforcement actions?

We are going to continue to see global investigations similar to the recent LIBOR and FX probes. With the SEC Enforcement Division's Financial Reporting and Audit Task Force and the recent arrival of Andrew Weissmann, who was a key player in the Enron Task Force, as Chief of the Fraud Section, there is the potential for a significant increase in accounting fraud enforcement actions. It will also be interesting to see how the Southern District of New York and other offices react to the Second Circuit's recent insider trading decision, *United States v. Newman*.

1 http://www.justice.gov/opa/pr/justice-department-recovers-nearly-6-billion-false-claims-act-cases-fiscal-year-2014

GSA'S PROPOSED TRANSACTIONAL DATA REPORTING RULE HAS SIGNIFICANT IMPLICATIONS FOR CONTRACTORS WITH GSA CONTRACT VEHICLES

By Tina D. Reynolds and Michael C. Mateer

On March 4, 2015, as part of an effort to reform its procurement process, the General Services Administration ("GSA") issued a proposed rule that would require GSA contract holders to report certain transactional data related to government orders placed against GSA contract vehicles, including the Federal Supply Schedule ("FSS") contracts, as well as other non-FSS contract vehicles. The same proposed rule would eliminate the "basis of award" customer and do away with the Price Reduction Clause found in FSS contracts. Earlier this month, GSA held a relatively rare public meeting on the proposed rule. In this Alert, we provide background on the proposed rule and details about the public meeting.

BACKGROUND

GSA administers a number of contract vehicles, including FSS contracts and non-FSS contract vehicles such as Governmentwide Acquisition Contracts ("GWACs") and Governmentwide Indefinite-Delivery, Indefinite-Quantity ("IDIQ") contracts (collectively, "GSA Contract Vehicles"). Through these GSA Contract Vehicles, companies can offer products for sale to federal government agencies (and other select public entities) at pre-approved prices and pursuant to pre-negotiated terms and conditions. GSA's goal in negotiating these contracts is to achieve for the government the same prices and terms as received by a company's most favored customer; or, at the very least, a fair and reasonable price.

In order to ensure the government customers receive the best possible price, GSA currently requires FSS contract holders to disclose extensive commercial sales practice ("CSP") information. FSS contracts also include a "Price Reductions Clause" ("PRC"). See 48 C.F.R. 552.238-75. The PRC requires that GSA and the contractor agree on a "basis of award" ("BOA") customer – that is, a customer (or category of customers) that receives from the contractor similar pricing and terms to those offered to the government. Thereafter, any discount or better term offered to the BOA customer must also be offered to government customers placing orders under the FSS contract. Failure to follow the PRC clause requirements or to extend these discounts to government customers can result in a breach of contract claim and/or False Claims Act liability.

THE PROPOSED RULE

On March 4, 2015, GSA issued a proposed rule that provides an alternative to the PRC and BOA customer tracking ("the

Proposed Rule"). See 80 Fed. Reg. 11619-01. Under the Proposed Rule, GSA would require that contractors provide transactional sales data related to FSS orders as well as orders under GSA non-FSS contract vehicles. Additionally, once implemented, FSS contract holders would not be subject to PRC or BOA requirements. They would, however, continue to be required to submit CSP data.

The Proposed Rule is part of GSA's move towards a "category management" style of procurement, in which the government shifts from managing purchases and prices individually, to managing entire categories of purchases across the government. In order to accomplish this transformation, however, GSA needs data on government sales. GSA determined it was too expensive to get that government sales data directly from the government customers, so it now proposes to obtain the data from FSS and non-FSS contractors. Contractors would be required to report data on sales of products and services placed GSA Contract Vehicles. The data to be provided includes, among other things, the purchasing entity, the price per unit, total price, quantity, manufacturer name, and part number. The contractor would enter the data monthly into an online reporting system. Contractors would not have to report on sales that occur through methods other than GSA Contract Vehicles.

For non-FSS contracts, many of which already contain some sort of data reporting requirement, GSA plans to implement the new clause immediately after adoption of a final rule. For FSS contracts, however, GSA would first test this transactional data approach through a pilot program. GSA would select certain schedules for participation in the pilot; participation by those schedule holders would be mandatory. GSA has indicated it would choose easily commoditized, high volume schedules for this test, including (preliminarily): Schedule 51V (Hardware Superstore), Schedule 58 I (Audio/Video); Schedule 72 (Furnishings); Schedule 73 (Food Service/Hospitality/ Cleaning); and Schedule 75 (Office Products/Services). After the pilot, GSA will evaluate its success by comparing discounts received under the pilot to various benchmarks. If successful, the pilot would be expanded to all FSS contracts; if a failure, GSA would return to the status quo.

PUBLIC MEETING

On April 17, 2015, GSA held a full-day public meeting on the transactional data reporting clause Proposed Rule. In short, there was a great deal of opposition to the rule change. Nearly all commentators – including the Inspectors General for GSA and the Department of Veterans' Affairs– had serious objections to the Proposed Rule, as written.

Below we summarize some of the more significant discussions from the April 17 meeting:

GSA's Presentation

GSA was represented by the Senior Procurement Executive, the Deputy Commissioner of the Federal Acquisition Service, and the Deputy Director of the Office of General Services Acquisition, and joined by the Administrator of the Office of Federal Procurement Policy. It presented the Proposed Rule and described the rationale behind it, as also set out in the Federal Register. A question and answer period followed. Significant questions included:

- **Freedom of Information Act:** There were concerns regarding how GSA would protect contractor transactional data from release under FOIA. GSA representatives stated GSA would attempt to protect unit price transactional data, but said that GSA would have to follow the normal FOIA processes. Furthermore, GSA indicated that in some cases it might reveal certain aspects of a contractor's transactional data as part of negotiations, to show other contractors if they were above or below market. GSA clarified, however, that it intended only to reveal a "competitive position," not the detailed data itself.
- **CSPs:** In response to questions, GSA indicated it had no intention of eliminating the CSP disclosures. It took the position that, especially without a PRC and BOA, it needs the CSP as a means to examine schedule holder's commercial transactions.
- **Tracking Complex or Non-Standard Products and Services:** A reoccurring theme throughout the meeting was how GSA intended to apply this transactional data model to complex products and services that were not necessarily comparable or competed only on price. GSA responded that it could track complex products and meaningfully compare them because it has "sophisticated" modeling capability. Furthermore, GSA indicated that it did not see why the Proposed Rule would lead to competition purely on price, as past performance information and product information would remain available to allow agencies to make selection decisions based on quality of the item or service.
- **Audits:** After implementation of the Proposed Rule, as part of its standard audit process, GSA would evaluate whether vendors properly provided all transactional data.
- **Requiring Contractors to Provide the Data:** GSA agreed that, in theory, it could acquire most if not all of the same data from Government agencies, but because this would require extensive updates to agency systems, software, etc., GSA thinks it is more expedient and cost effective to require industry to gather the data.

Inspectors General

Both the GSA Inspector General's Office, represented by the Program Director of the Office of Audits, and the Veterans' Affairs Inspector General's Office, represented by the Counselor to the Inspector General, were against the Proposed Rule as written. The GSA OIG had four areas of concern:

- **Elimination of PRC.** The representative of the GSA OIG expressed the GSA OIG's belief that elimination of the PRC will eliminate significant incentives for vendors to provide the Government with discounts. The GSA OIG refuted GSA's evidence that purports to show the ineffectiveness of the PRC, and suggested that GSA would have to do a broader study of how much money the PRC saves the government before GSA could determine if the PRC was more or less effective than the Proposed Rule.
- **Divorce from Commercial Pricing.** The GSA OIG is concerned that elimination of the PRC and BOA would divorce the government schedule price from commercial pricing, and result in the government paying more than commercial customers. Continuing the CSP process, together with additional efforts to gather separate commercial sales data could mitigate this concern, but not entirely.
- **Burden of Reporting.** The GSA OIG believes GSA is underestimating the burden to contractors and the government in reporting this data. Contractors would likely spend more time than GSA estimates. Additionally, GSA would have to create a system to collect the data, and mechanisms for enforcing the new rule, which the GSA OIG believes GSA has not fully taken into account when describing the costs of the Proposed Rule.
- **Non-Standard Products/Services.** The GSA OIG highlighted the difficulty in comparing non-standard products and services. Any product or service that cannot be effectively standardized will break the model. The GSA OIG does not have GSA's confidence in its ability to track and compare such products and services.

The representative of the VA OIG expressed similar concerns, and added, among other things, that if GSA eliminates the PRC, the VA OIG believes the Economic Price Adjustment clause should also be modified or eliminated. Otherwise, the Economic Price Adjustment clause would allow schedule prices to grow out of control, unchecked by a BOA.

Industry

Industry representatives included the Coalition for Government Procurement and the National Defense Industrial Association. Industry representatives objected to the cost and necessity of the Proposed Rule, as well as the lack of protection for contractor data. Industry offered alternative ideas to GSA, including a suggestion that it gather the transactional data from government customers (building a new system to do so, if necessary) or that it scrap both the PRC and the Proposed Rule, and simply rely upon the competitive process to result in fair pricing.

Conclusion of Public Meeting

GSA indicated that the commentary had raised some concerns, particularly the opposition of the GSA and VA OIGs, as well as industry's worry that GSA is underestimating the burden of the reporting process. GSA emphasized, though, that the FSS project would begin with a "pilot." Further, GSA indicated that the choice for the FSS still seems to be between "the Devil we know [PRC], or the devil we don't [transactional data]."

We will continue to monitor ongoing developments and to work with our clients to ensure that their contract reporting meets all regulatory requirements.

INTERNATIONAL IT COMPANIES FACE CONTINUING HEADWINDS IN CHINA

By Paul D. McKenzie and Gordon A. Milner

Our September 16, 2014 client alert, "Brave New World? Recent Challenges Facing Foreign IT Companies in China," discussed efforts by the Chinese government to enforce heightened network security standards, with a particular focus on the issuance on September 1, 2014 by the Ministry of Industry and Information Technology ("**MIIT**") of the Guiding Opinions on Strengthening Network Security in the Telecommunications and Internet Sectors (关于加强电信和互联网行业网络安全工作的指导意见; the "**MIIT Opinions**").

A great deal has happened since the MIIT Opinions were issued. Developments include:

- the announcement of network security standards in the banking sector that have raised substantial concerns for both financial institutions and IT providers, including a growing concern among foreign IT companies ("**FITCs**") that the Chinese government's campaign to enhance network security is a thinly disguised "buy local" campaign; and
- the circulation of a draft Anti-Terrorism Law that contemplates Chinese government agencies being given very far-reaching powers to access data transmitted over the Internet and other telecommunications networks.

This client alert outlines these key developments and discusses their potential impact on FITCs.

BANKING STANDARDS – EVIDENCE OF A GROWING "BUY LOCAL" CAMPAIGN?[1]

The banking sector appears to be at the vanguard of the Chinese government's network security campaign. Network security standards announced to govern the banking sector have potential significance far beyond that sector, since it seems likely that the experience implementing these new standards will inform the regulatory approach in introducing network security standards in other sectors in the future.

These banking standards reflect a clear distrust of the security of foreign IT products and services. They almost certainly also represent an effort by the Chinese authorities to help local products and services move up the IT value chain and reduce dependence on foreign IT. FITCs are reasonably concerned that their market access in China will be adversely affected.

On September 3, 2014, the China Banking Regulatory Commission ("**CBRC**"), the National Development and Reform Commission, the Ministry of Science and Technology, and MIIT issued the *Guiding Opinions Regarding Application of Secure and Controllable Information Technologies to Strengthen Network Security and Informization of the Banking Sector* (关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见; the "**Banking Opinions**").

The Banking Opinions encourage the use of "secure and controllable" (安全可控性) information technologies – adopting the same term that appears prominently in the MIIT Opinions and other government documents – and call for implementation of network security review standards for the banking sector. Other key provisions include the following:

- Specific goals for utilization of secure and controllable technologies in the banking sector are set: 15 percent in 2015 and no less than 75 percent in 2019.
- The importance of developing local technology is emphasized.
- Priority is given to technologies and solutions that are "highly open, highly transparent and of a broad application scope" and to suppliers who are willing to work on a cooperative basis in relation to key knowledge and critical technologies.

The Banking Opinions were followed by issuance by the CBRC and MIIT on December 29, 2014 of the following:

- *the Implementing Guideline for Promoting the Application of Secure and Controllable Information Technology in the Banking Sector* (2014–2015) (银行业应用安全可控信息技术推进指南(2014–2015年度; the "**Guideline**"), which is appended with
- *the Classification Catalogue of Banking Information Technology Assets and Security and Controllability Targets for the Banking Sector* (银行业信息技术资产分类目录和安全可控指标; the "**Catalogue**").

The Guideline and Catalogue implement the Banking Opinions by defining specifically what "security and controllability" require in regard to stipulated categories of IT products and services. The Catalogue covers a very wide range of products and services in considerable detail – specifically addressing some 50 sub-categories of hardware (ranging from mainframes, through specialized banking hardware like ATMs to fungible items like printers), 12 sub-categories of software (including operating systems and office software in addition to specialized banking applications), and 6 types of technical services (including consulting, development, and outsourced operations). For each sub-category, the Catalogue sets out "security and controllability" criteria together with minimum utilization rates to be achieved in 2015.

The Guideline specifies that it applies to all banking financial institutions established within the PRC. We understand that the term includes commercial banks as well as policy banks, financial asset management companies, and other financial institutions under the direct supervision of the CBRC and does not include, for example, international trust and investment companies, which are not under CBRC supervision. For the balance of this Alert, we use the generic term "bank" to refer to banking financial institutions governed by the Guideline.

It is beyond the scope of this Alert to discuss in detail the specific criteria for being secure and controllable for each category of IT product and service. However, criteria that are causing FITCs concern about their continuing access to the Chinese market include the following:

- For all of the various categories of software product and (in respect of firmware and embedded software components) many of the categories of hardware products listed in the Catalogue, source code is required to be submitted to the CBRC. Many vendors consider the source code to their products to be highly sensitive for both intellectual property protection and security reasons and have historically declined to file source code with public authorities even at the cost of missing out on the enhanced protection afforded under the existing voluntary Chinese copyright registration regime for source code. As such, the requirement for mandatory submission of source code has caused particular

concern among FITC vendors. It appears that those concerns are at least partially recognized by the CBRC. In a notice on February 12, 2015, the CBRC commented that the details of the requirement to submit source code are still being investigated and will be implemented only after "various opinions have been heard."

- The embedded software (and, in some cases, hardware chips) used in almost all sub-categories of networking, storage, and security hardware is required to be "under indigenous IPR." Notes to the Catalogue explain this requirement as meaning that the intellectual property in those components must be either exclusively owned and controlled by a Chinese party or used by a Chinese party under long-term rights without restrictions on innovation. Further clarification will be required from the CBRC, but on its face, this requirement could force FITC vendors to produce separate "China-only" versions of their product lines and could make it extremely difficult for foreign banks to maintain globally standardized networks.
- Trusted computing modules utilized in various types of computer equipment must be those that have obtained certification as commercial encryption products in China – meaning in effect that they may not utilize the international TPM standard, which is not currently certified in China, and must use the Chinese TCM standard.
- All categories of IT hardware and software listed in the Catalogue are subject to the vague requirement that "technology risk and supply chain risk are controllable." Some commentators have suggested that this may be construed as requiring that relevant products be manufactured in China. This may be an overly conservative interpretation – though it is worth noting that many FITC products are, as a matter of fact, already manufactured in China.
- Suppliers of almost every category of IT hardware and software listed in the Catalogue are required to operate R&D and service centers within China, "providing continuous upgrades and technical support services" for products. While many major FITCs already possess facilities in China, those who do not will need to decide whether to establish local affiliates. From the point of view of the banks, this has the potential to cause problems for the use of foreign-developed open source products – a point which will need to be clarified by the CBRC.
- A number of categories of IT product are subject to testing and certification requirements, without explaining the nature of the testing or identifying the certifying organization.

The benchmarks for minimum utilization vary significantly with the category of product or service. Perhaps reflecting the difficulties in replacing specialized software, the lowest rates (5, 10, or 15 percent, depending on the category of bank) apply only to procurement of "dedicated" banking software. A 100 percent rate applies to most categories of computer hardware and to all categories of security equipment, which may reflect the more fungible nature of such equipment.

The Guideline specifies in considerable detail the work that banks are expected to undertake to implement the requirements of the Guideline and Catalogue and the work of both CBRC and MIIT to support and evaluate banks in their implementation. It also sets out a March 15 deadline for each bank to submit a report to CBRC addressing matters such as the management organization it has put in place to oversee implementation of the Guideline and Catalogue. The Guideline also encourages banks and IT companies to bring to the CBRC's attention difficulties and questions they encounter in regard to testing and certification and other requirements and provides that CBRC and MIIT will be equipped to start receiving from IT companies relevant filings and risk evaluation requests contemplated under the Catalogue beginning April 1, 2015.

DRAFT ANTI-TERRORISM LAW

On November 3, 2014, the National People's Congress ("**NPC**") issued the Anti-Terrorism Law (First Review Draft) (反恐法草案(一审稿)) for public comments.

The first draft of the law caused significant concerns among FITCs due to the following requirements:

- In their design, construction, and operation of telecoms and internet networks, telecommunications network operators and internet service providers must "preset" a technical interface and submit the encryption scheme with the authority responsible for encryption – vague language that commentators understand to mean that PRC government authorities would have broad rights to monitor network use.
- Telecommunication services providers and internet service providers must keep relevant equipment and data in respect of local users within the territory of China.

According to March 9, 2015 comments made by a representative of the legislative drafting committee of the NPC Standing Committee, a review of a second draft of the law was completed in February and, while the law is not on the agenda for the NPC session that convened on March 5, 2015, the law may undergo third reading and promulgation later in 2015.

In responding to questions about the draft law, spokesperson for the NPC, Fu Ying, is quoted by Xinhua news agency as stating that the second draft of the law

stipulates that use of the technical interface (1) is limited for purposes of investigating and preventing terrorist activity, (2) is limited to public and state security agencies, and (3) is subject to a strict review and approval process.

OTHER DEVELOPMENTS IN REGARD TO NETWORK SECURITY

Network Security Convention

We have learned from an industry source that, on December 2, 2014, the National Information Security Technology Standardization Technical Committee of the China Communication Standards Association (中国通信标准化协会网络与信息安全委员会; "**NIST**") and China Information Security Certification Center (中国信息安全认证中心; "**ISCCC**") jointly distributed a Self-Discipline Convention on Safeguarding User's Network Security by Information Technology Product Suppliers (信息技术产品供应方维护用户网络安全自律公约; "**Convention**") to a limited circle of IT companies, who were invited to be founding signatories to the Convention.

The initial draft of the Convention covers a wide range of IT products and services, including hardware, software, systems, and services having capabilities that include storage, processing, transmission, control, exchange and display of information or data, including computers and peripherals, communications equipment, network equipment, automatic control equipment, operating systems, databases, application software, and services.

It includes covenants relating to collection, storage, and use of both personal data and information related to the State.

One key focus of the draft Convention is the control of remote control interfaces (sometimes known as "backdoors") in IT products. Specific covenants in regard to network security include the following:

- Remote control of user products is allowed only to the extent required for product maintenance or other purposes. Users must be expressly informed of the purpose of remote control and the ports and protocols used. Users should have the ability to disable remote control and be informed of the loss of function if they do so. Express consent of users is required for remote control, and users must be provided with real-time information about the status of remote control.
- Products should not include a covert interface or any module without an express function and components should not be installed that can disable or bypass security mechanisms. Any interface for testing or maintenance should be disclosed to users and should be capable of being shut down by users.
- Users should have the ability to schedule remote control, and records of data input and output during the remote control process should be maintained.
- In necessary cases, IT product suppliers should provide a relevant government-accredited third-party institution with the method and evidence that can be used to test and verify activity, such as collection of user information and remote control of user products.

Recent inquiries with officials at ISCCC suggest that the Convention has not yet been signed and may be subject to revision.

Health Care Measures

In May 2014, the National Health and Family Planning Commission issued the Administrative Measures on Management of Population Health Information (人口健康信息管理办法(试行); the "**Measures**").

The Measures contemplate relatively detailed restrictions on the collection, storage, and utilization of personal health information by various categories of health care providers, including a prohibition on the use of servers outside China for the storage of such information.

Interestingly, the Measures provide that all IT products on China's health care IT systems must obey the "national network security review regime," without specifying what that review involves, providing further evidence, if evidence is needed, that the Chinese government continues to work toward a network security review regime that reaches beyond merely the banking sector.

LOOKING FORWARD

The Chinese government has signaled clearly and repeatedly its commitment to increase network security, and so FITCs cannot expect related market access problems to abate – quite the opposite.

The coming weeks will see banks in China scrambling to understand the requirements of the Guideline and Catalogue, FITCs and domestic IT suppliers seeking to qualify their product offerings, and intense lobbying by banking institutions and IT suppliers, as well as by the United States, the European Union, and other foreign governments for an easing of the requirements.

Foreign banks operating in China will already have had to submit initial reports to their local CBRC offices in respect of the implementation of the Guideline and Catalogue. The new rules will cause a major headache for banks that have spent recent years seeking to optimize efficiency and security by standardizing IT hardware, softwares and networks across their global organizations. The integration of novel, locally developed Chinese systems into a bank's global IT systems may itself trigger further regulatory testing and approval requirements from the bank's overseas regulators. Moreover, the difficulties of implementing potentially major and intricate changes to

banks' China IT systems may be exacerbated if the FITC consultants and system integration providers that helped build the banks' existing systems gradually elect to cede the market to local providers.

Meanwhile, Chinese regulators will likely turn their sights to network security beyond the banking sector. In its *Twelfth Five-year Plan for Information Security Industries (2011 to 2015)* (信息安全产业"十二五"发展规划), MIIT identified e-government, e-commerce, e-healthcare, finance, energy, transportation and distance education as sectors where use of secure and controllable IT products and services should be enhanced. Some of these sectors may soon be the target of sector-specific efforts. We also expect that efforts to implement the broader "cyber security review" regime that PRC government officials proposed (see our September 2014 client alert) will continue.

At this stage, it is unclear to what extent the detailed provisions of the Guideline and Catalogue in respect of the banking industry will guide future, more generally applicable legislation. Many of the sub-categories of products identified in the Catalogue are rather generic, and many of the criteria applied to those categories might easily be adopted in other sectors or in a broader cybersecurity review regime. At the least, it is not difficult to see the same arguments that were made for imposing the restrictions on the banking industry being made in respect of some other industries, and so we anticipate that the discussions and lobbying in regard to the Guideline and Catalogue that are currently underway will have ramifications beyond the banking sector.

WHAT THIS MEANS – NEXT STEPS FOR FITCS

The rather vague and open-ended language used in the Guideline and Catalogue makes it difficult for FITCs to plan ahead. However, it is possible to identify several steps that FITCs will need to consider:

i. **Assess the risk.** FITCs will need to review the products and services they offer to banks in China in order to assess and quantify the risks inherent in complying with the Guideline and Catalogue (for example, the IPR risks involved with disclosing sensitive source code or the security risks inherent in replacing software with indigenously sourced alternatives).

ii. **Assess the costs of localizing.** FITCs supplying almost every category of IT hardware and software listed in the Catalogue are required to operate R&D and service centers within China. Many FITCs will need to establish new PRC subsidiaries or repurpose their existing onshore affiliates in order to comply with this requirement. Doing so may require a material investment in capital and management time.

iii. **Assess the market.** FITCs will need to consider whether the value of the China banking market justifies the risk and costs identified under steps (i) and (ii). It may be that the banking sector constitutes a relatively small market segment for many FITCs. The cost-benefit analysis would look very different if the rules are generalized to other industries.

iv. **Identify procedures.** FITCs will need to identify the procedures involved in qualifying their products and services with CBRC and other relevant regulators. Some of these procedures already exist, and FITCs should seek advice from specialist, experienced counsel. Other procedures (for example, filing source code with CBRC) have not yet been established, and it may be sensible for FITCs to consider working with trade associations (see below).

v. **Consider forking.** In order to comply with the source code disclosure, indigenous innovation, and other requirements, we anticipate that some FITC vendors will seek to "fork" their product lines, creating specific versions for China that are likely, over time, to evolve away from the product lines used for the rest of the world.

vi. **Work with trade associations.** Many FITCs are working closely with the China chapters of international trade associations (for example, United States Information Technology Office, also known as "USITO") to stay abreast of the latest pronouncements from the CBRC and other relevant China regulators. In addition to disseminating information, such organizations have been seeking to engage the Chinese government in dialogue regarding how the Guideline and Catalogue will be interpreted and how best to implement key procedures (such as source code filing) in a manner that takes into account the legitimate concerns of FITCs.

1 In a notice that was issued in mid-April, the China Banking Regulatory Commission announced the suspension of implementation of the Banking Opinions. It remains unclear what network security standards may be implemented in place of the Banking Opinions and what the timetable is for implementation of any such other standards. The Banking Opinions nonetheless remain a valuable guide regarding the thinking of regulators in relation to the network security of various types of information technology products and services.