LEGAL ADVISOR

A PilieroMazza Update for Federal Contractors and Commercial Businesses

Business & Corporate Law

REGULATORY ISSUES FOR ACQUISITIONS OF GOVERNMENT CONTRACTS BY NON-U.S. BUYERS

By Kimi Murakami

With the uptick in M&A transactions for government contractors, we have seen an increase in cross border transactions. There are several unique regulatory regimes that must be analyzed when structuring M&A transactions involving the purchase by a non-U.S. buyer of a company that performs federal government contracts or the acquisition of certain assets that include government contracts. Failure to address these issues at the onset of a deal can lead to devaluation of the target, at best, and rescission or unwinding of a transaction, at worst. This article outlines some of the key questions when structuring the acquisition of government contracts by a nondomestic buyer.

Do the government contracts involve classified information?

If the government contracts at issue involve classified information, the target company has a facility clearance (FCL) to perform the work. To obtain its FCL, the company must have certain procedures in place as required by the National Industrial Security Program Operating Manual (DoD 5220.22-M, Feb. 2006) (NISPOM) issued by the Department of Defense. Under the NISPOM, as soon as substantive negotiations between the seller and a buyer are underway, notification must be given to the target company's Cognizant Security Agency (CSA). If the acquisition will be structured as a stock purchase where the contractor continues as a subsidiary of the buyer, the target company's clearance will continue with the CSA's approval. The parent company is also required to have an FCL at the same or higher level as the subsidiary.

The fact that an international buyer is a company under foreign ownership, control or influence (FOCI) presents a potential regulatory snag when acquiring a contractor with an FCL.

The fact that an international buyer is a company under foreign ownership, control or influence (FOCI) presents a potential regulatory snag when acquiring a contractor with an FCL. Companies under FOCI cannot hold an FCL unless FOCI is negated or mitigated to the satisfaction of the CSA. Mitigation measures must be put in place in order to insulate the classified information that the target company has access to as the holder of an FCL from the non-U.S. buyer for national security purposes. The mitigation methods that can be employed range from board resolutions of the target company, voting trust agreements, proxy agreements, a special security agreement, or a security control agreement depending on the facts of the case.

To CFIUS or Not to CFIUS?

At the same time the parties engage in an analysis of the issues described above relating to classified work, consideration of the national security impact of the transaction should also

Continued on page 2

In This Issue

Published by

PILIERO MAZZA PLLC
ATTORNEYS AT LAW

FOREIGN ACQUISITIONS . . . . . .

Continued from page 1

begin. The U.S. government through the Executive Branch has the authority to review all mergers, acquisitions, and takeovers that could result in foreign control of persons engaged in interstate commerce under the authority of the Exon-Florio Amendment (Section 721, Defense Production Act of 1950, as amended (50 U.S.C.App. 2170)) (Exon-Florio). Exon-Florio provides for the review of these transactions by the President to be initiated through notice to the Committee on Foreign Investment in the United States (CFIUS). CFIUS is an intergovernmental agency comprised of senior representatives of twelve agencies of the U.S. government including the U.S. Departments of Treasury, Homeland Security, Commerce, Defense, State, and Energy. CFIUS is only concerned with "covered transactions" as defined under Exon-Florio which are transactions in which a U.S. business will be acquired by a foreign buyer or that will result in the foreign buyer having control over a U.S. business.

Filing for CFIUS approval is voluntary. As a result, some parties may suggest skipping this step to save time, expense, and hassle. Skipping CFIUS review is a calculated risk because it leaves open the possibility that the U.S. government could initiate its own review of a transaction at any time. If a transaction involves cleared facilities (see above) or export controlled defense articles (see below), obtaining clearances or licenses in the future could be more challenging and subject to increased scrutiny if the transaction has not been cleared by CFIUS. Therefore, in most transactions involving non-U.S. buyers, the most prudent approach is to file for the CFIUS review.

CFIUS review begins by filing a joint voluntary notice of the proposed transaction no later than five business days prior to the formal filing. Upon receipt of a formal filing, CFIUS will conduct a 30-day review and, in most cases, determine that a full investigation is not warranted. If the transaction raises significant national security issues, CFIUS will undertake a more thorough 45-day investigation. After that review, CFIUS will determine whether the transaction can go forward or should be sent to the President to decide whether the transaction can proceed. Parties should factor these timelines into the transaction schedule.

Does the target company hold export control licenses?

If the target company exports items related to defense or national security, it must comply with the International Traffic in Arms regulations (ITAR) administered by the U.S. Department of State. To be ITAR compliant, the contractor must register with the Directorate of Defense Trade Controls (DDTC). Under the ITAR, a registrant must notify the DDTC at least 60 days in advance of the intended sale or transfer of ownership or control to a foreign person. The other export-import regime in the U.S. is administered by the Department of Commerce and governs dual use items that have both commercial and military functions under the Export Administration Regulations (EAR). Items that fall under EAR are listed on the Commerce Control List. If subject to ITAR and EAR, post-closing change of ownership notifications and registrations must be carefully observed and completed.

Consideration of the foregoing issues is critical for a non-U.S. buyer to continue performance of acquired federal government contracts and realize the contemplated value of the acquisition. Getting the most value for the company and its assets including government contracts is of utmost concern for the seller as well. Favorable resolution of the regulatory issues raised above, therefore, will be a win-win on both sides of the deal table at closing.

About the Author: Kimi Murakami is counsel with PilieroMazza and focuses her practice on corporate transactions with an emphasis on mergers and acquisitions for government contractors. She can be reached at kmurakami@pilieromazza.com.

Small Business

NOW IS THE TIME FOR GOVERNMENT CONTRACTING REGULATORY COMPLIANCE REVIEWS

By Patrick Rothwell

Twice a year, at the time our clocks are set forward for daylight savings time and set backwards to standard time, we all get reminders from the fire department or the television news that we should test and change the batteries of the smoke and carbon monoxide detectors in our homes. Similarly, the New Year is a good time for small government contractors to check their compliance

programs to make sure they are still working. This article offers suggestions for a compliance review that would be manageable and beneficial to ensure your compliance program works well this year.

To begin, firms that pursue federal small business set aside procurements should review, at the start of each new year, their federal tax returns, books of account, and internal financial statements and estimates for the last three completed fiscal years (as well as payroll records for the past 12 months) to determine whether they are near or over the SBA size standard(s) applicable to any small business set aside procurements which they may seek this year. Once the prior year ends, that year must now be included in your calculation of small business status. Therefore, it is important to assess as early as possible in the New Year how the most recently-completed year will impact your small business status.

It is a common misconception that until a concern files a federal income tax return for its most recently completed fiscal year, its size is measured by the prior three fiscal years for which there are completed federal income tax returns. In fact, size is always measured based on the three most recently completed fiscal years (or the last 12 months for employee-based size standards). Until you file your tax returns for the most recently-completed year, SBA will use any other available information to calculate your firm's receipts for that year, including regular books of account, audited financial statements, and affidavits. SBA may also use your tax returns once they are filed later in the year. Thus, you cannot wait until you file your tax returns. You need to consider early in the New Year whether, based on your financial statements and estimates for the past year, that year will bump you over the size standard for your industry. While a mistaken self-certification of size may be inadvertent, there is, besides the potential loss of a contract, always the risk that SBA might consider the concern's self-certification to be a false certification, which would compound the consequences.

The New Year is also a good time for contractors to review their System for Award Management (SAM) profile. The FAR generally requires that contractors, in order to keep their SAM registrations active, review and update on an annual basis the information contained in their SAM profiles to ensure they are current, accurate and complete. Although the annual update requirement may take place at a different time during the year, it is a good idea for a contractor to get into the habit of performing this review early in the New Year to ensure your SAM profile is current, accurate, and complete.

Small contractors should also set aside time in the New Year to review their profiles on other databases which have information about the company, including its business relationship and even its relationship with individuals. Among the profiles that should be reviewed include the contractor's SBA Dynamic Small Business Search database profile (if it has one), its Dun & Bradstreet report, its LinkedIn profile, its website, and any other similar source of information available to the public. A disappointed bidder may well use any information contained within such databases, including SAM profiles, as a basis to allege that a particular concern is other than small. Such information could include the contractor's purported number of employees, its supposed revenues, its business or other relationships that could allegedly give rise to an affiliation allegation, and much else that could be misconstrued. Therefore, it is important that the information contained in these databases be current and accurate, so that a competitor does not use inaccurate or outdated information as a basis to challenge a contractor's size.

Finally, the New Year is a good time for a contractor to review and update, if needed, its Code of Business Ethics and Conduct. With certain exceptions, a concern which has a federal contract, the value of which is expected to exceed $5.5 million and the performance period of which is 120 days or more, is required to develop a Code of Business Ethics and Conduct. If you do not have an Ethics Code, make a resolution to put one in place this year. If you already have one in place, spend some time in the New Year to review your Ethics Code to make sure it is realistic and up-to-date with your current business practices and the ever-changing regulatory and compliance landscape for small contractors. You should also be aware that if your firm has a federal contract that is not for a commercial item and for which your firm has not represented itself as a small business, you are also required to develop an ongoing business ethics awareness and compliance program and internal control requirements that comply with the standards in the FAR. If you have an ongoing ethics compliance program and internal controls, it is particularly timely for you to review them now to make sure that they both meet the standards set forth in the FAR and the particular needs of your firm.

While most of this work can and should be performed internally by the federal contractor, PilieroMazza has regularly been asked by clients to provide assistance with government contracting regulatory compliance issues, such as reviewing the contractor's size or its code of business and ethical conduct. We would be happy to be of assistance should your business find that outside assistance from legal counsel in performing government contracting compliance reviews is warranted.

About the Author: Patrick Rothwell, an associate with PilieroMazza, practices primarily in government contracts and litigation. He can be reached at prothwell@pilieromazza.com.

GUEST COLUMN

The Guest Column features articles written by professionals in the services community. If you would like to contribute an original article for the column, please contact our editor, Jon Williams at jwilliams@pilieromazza.com.

SUPPLY CHAIN CYBERSECURITY RISK IN GOVERNMENT CONTRACTING

By Jason Clark, ISMS Solutions

The digital superhighway is young, relatively unregulated and functions like the Wild West where both public and private sector organizations are experiencing avoidable breaches in their data due to the fact that their information security management systems are incomplete or absent. Implementing adequate cybersecurity controls is an immediate necessity as the cost and effort in developing, implementing and monitoring solid information security practices could be dwarfed by the cost of remediating a major security breach.

It is not just your organization's infrastructure that needs oversite as some of the largest data breaches were perpetrated by hackers gaining entry via third party vendors. Understanding your supply chain's cybersecurity has become critical in defense contracting because on October 30, 2015, the Department of Defense (DoD) issued a Final Rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) which allows the DoD to mitigate supply chain risk by: 1) excluding sources of supply from covered procurements for failing to meet qualification standards or for failing to satisfy evaluation factors; or 2) withholding approval for prime contractors to use certain subcontractors.

While still largely unregulated, the U.S. government, in an effort to protect against attacks, is using its powers to enforce compliance with measures that are constantly evolving. This creates a nightmare scenario as inadequate cybersecurity management systems can have numerous adverse consequences for federal government prime and subcontractors involved in the development or delivery of information technology products and services related to National Security Systems including:

- Cessation of current contracts and inability to win new business
- Loss of proprietary information and data
- Damage to reputation
- Resources needed to remediate the problems

Soon, even more government agencies will require all of your corporate partners, suppliers and data providers to meet specific security levels in order to maintain or retain business for fear of data breaches. Therefore, cyber hygiene across your supply chain is the only antidote to an already infected business population.

Going forward you need to ask your supply chain partners questions such as:

- Does your organization have a process in place for handling and mitigating issues with your information security program?
- Does your organization have a set of information security policies to cover acceptable use, access control, supplier management and incident management policies?
- In the last 12 months has your organization conducted a comprehensive internal audit to look at the effectiveness of your security controls and has top management reviewed the results?
- Does your organization have a policy of encrypting transfers of critical data?
- In the last 12 months has your organization completed a vulnerability scan on network(s) and computing systems?
- Has your organization clearly identified regulatory, statutory, and contractual information security and privacy requirements?
- What type of data does the supply chain partner handle on your behalf and what type of access do they have to your infrastructure?

Knowing the answers to these and other questions will help determine the risk each supply chain partner poses to your government contracts. Once you understand this risk, the next step is to determine the level of compliance you will require from your supply chain partners. For example, will you require that your supply chain partners to have ISO 27001, NIST, HIPPA, some other security certification or that they match your company security standards? Lastly, you will need to track and verify their compliance on an ongoing basis.

All of this probably sounds quite daunting in terms of procedural know-how and level of effort, but there are products and services, such as ISMS' Conformance Works,

which allow organizations a central, online location to manage their own vendor network and to aggregate, authenticate and enhance the level of compliance of their supply chain partners.

Being secure should be every organizations goal. However, in this day and age your corporate partners must also be secure in order to avoid potential disaster so knowing their level of cybersecurity is as important as knowing your own.

About the Author: Jason Clark is the President and Founder of ISMS Solutions (www.ismssolutions.com), a management consulting firm that employs a holistic, organized approach to addressing governance, risk management, and compliance (GRC) strategy and implementation. Specializing in information security, ISMS collaborates with clients to customize, implement and automate information security standards and processes that meet or exceed certification standards. ISMS also has a proprietary information security platform, Conformance Works, which allows clients to manage customized risk and compliance initiatives across their organizations, as well as vendors and other associated companies. He can be reached at jclark@ismssolutions.com.

Labor & Employment Law

DOL'S CHANGES TO THE OVERTIME RULES IN 2016 MEAN EMPLOYERS MUST REEVALUATE WHETHER EMPLOYEES ARE ENTITLED TO OVERTIME

By Corey Argust

The Fair Labor Standards Act (FLSA) is quite possibly the labor law that employers grapple with more than any other. The regulations can be murky at best when actually applied and the price tag for running afoul of the regulations is staggering. Aside from the ever-vigilant and watchful eye of the Department of Labor (DOL), employers continue to face increased scrutiny and potential liability for FLSA violations in private lawsuits. Between 2011 and 2014, the number of FLSA lawsuits increased more than 19%. In a similar vein, workplace class and collective action settlements rose to an all-time high of $2.48 billion in 2015, a 33% increase from the previous year. A great majority of these lawsuits stem from the misapplication of the rules regarding overtime exemptions or failure to properly pay overtime.

The bad news is that more change is coming in 2016. The DOL is set to release new overtime regulations in the coming months and employers will need to evaluate whether any employees will be entitled to overtime under the changes to the overtime rules. The good news is that these changes are an opportunity for businesses to get a solid handle on the overtime rules overall *and* smoothly make any necessary adjustments to current practices, regardless of whether those adjustments directly relate to the new regulations. The changes to the overtime rules are explained below followed by steps that employers should take to avoid liability for overtime violations.

You might recall that in 2014 President Obama directed the DOL to develop new regulations to modernize and streamline the FLSA overtime exemptions for executive, administrative, and professional employees. These regulations would govern whether such "white collar" employees are entitled to overtime pay. On June 30, 2015, the DOL released its Proposed Rule, which would increase the current minimum salary for white collar employees from $455 per week (or $23,660 per year) to a minimum of approximately $970 per week (or $50,440 per year), a 113% increase to the salary threshold requirement. Under this change, the DOL estimates that almost five million additional white collar employees will be entitled to overtime pay.

Under the FLSA, employers generally must pay employees overtime—that is, pay at a rate of one and one-half times an employee's regular pay rate for every hour that the employee works in excess of 40 hours per week. Employers are excused from paying overtime only if an employee qualifies for a specific exemption from the FLSA's overtime pay provisions. Some of the most commonly used and misapplied overtime exemptions are those for executive, administrative, and professional employees. To qualify for these white collar exemptions, employees must meet the requirements of the "duties" test and a "salary" test.

In recent years, the minimum salary necessary to meet the salary threshold for the white collar overtime exemptions has remained relatively low. Because of the low salary threshold, many employers have applied the exemptions without also carefully examining whether, under the duties test, employees' duties are supervisory, entail non-manual work involving managerial of business operations or exercise independent judgment and discretion in matters of significance to the employer. The DOL has not failed to notice the difficulties employers face in determining the applicability of the white collar exemptions and, in no uncertain terms, has made clear that the investigation and prosecution of overtime violations is, and will continue to be, one of its top priorities.

Moreover, the upcoming changes to the overtime rules are likely to affect the applicability of the Service Contract Act (SCA) to government contracts or employees working on those contracts. The SCA is intended to apply to service employees that are paid hourly and excludes those white collar employees as defined by the FLSA exemptions. As employees on an SCA contract shift from exempt to non-

Continued on page 6

PILIERO MAZZA PLLC
ATTORNEYS AT LAW
888 17th Street, NW, 11th Floor, Washington, DC 20006

PRSRT STD
AUTO
U.S. POSTAGE PAID
WASHINGTON, DC
PERMIT NO. 1976

The Legal Advisor newsletter is published by PilieroMazza PLLC, a law firm that provides legal services to commercial businesses, federal contractors, trade associations, Indian tribes, Alaska Native Corporations, and other entities. If you have any comments or suggestions for future articles, please contact our editor, Jon Williams, at jwilliams@pilieromazza.com.

CHANGES TO OVERTIME RULES . . .

Continued from page 5

exempt, they will also be entitled to the prevailing wage and benefits of the applicable wage determination. Additionally, if a significant number of employees working on a government contract shift in classification from exempt to non-exempt employees due to the change in overtime rules, the SCA may well become applicable to that government contract if those employees perform the work of "service employees."

What does all of this mean for employers? The DOL's Final Rule revising the salary threshold will likely be published by mid-year and become effective within 60-90 days after publication. This is not much time to come into compliance. Employers should take the opportunity between now and the publication of the Final Rule to fully evaluate whether employees currently classified as exempt from overtime in fact meet *both* the duties test and salary threshold requirement. If employers currently have employees misclassified as exempt, now is an opportune time to bring your company into compliance by appropriately reclassifying employees. Further, employers should take the opportunity to evaluate whether it makes economic sense to raise the salaries of employees falling just below the salary threshold, but otherwise meeting the duties test, to maintain exempt status.

With these suggestions in mind, the following are best practices for conducting an internal FLSA audit:

1. Carefully review all exempt salaried positions to determine whether the positions meet the applicable duties test;
2. Evaluate whether the increase in the salary basis test will affect any classification;
3. Implement any necessary changes to your timekeeping and overtime approval policies or practices;
4. Ensure all deductions from salary are permitted under the regulations;
5. Assess the cost impact of any changes in classification of the affected employees or the government contract, if applicable; and
6. Seek guidance from legal counsel trained to assist with FLSA classification analysis.

By conducting a thorough FLSA audit now, employers will be prepared for the upcoming changes and position themselves well to avoid the costly liability that could result from a DOL audit or overtime lawsuit.

About the Author: Corey Argust, an associate with PilieroMazza, practices in the areas of employment law, litigation and govenment contracts. He can be reached at cargust@pilieromazza.com.