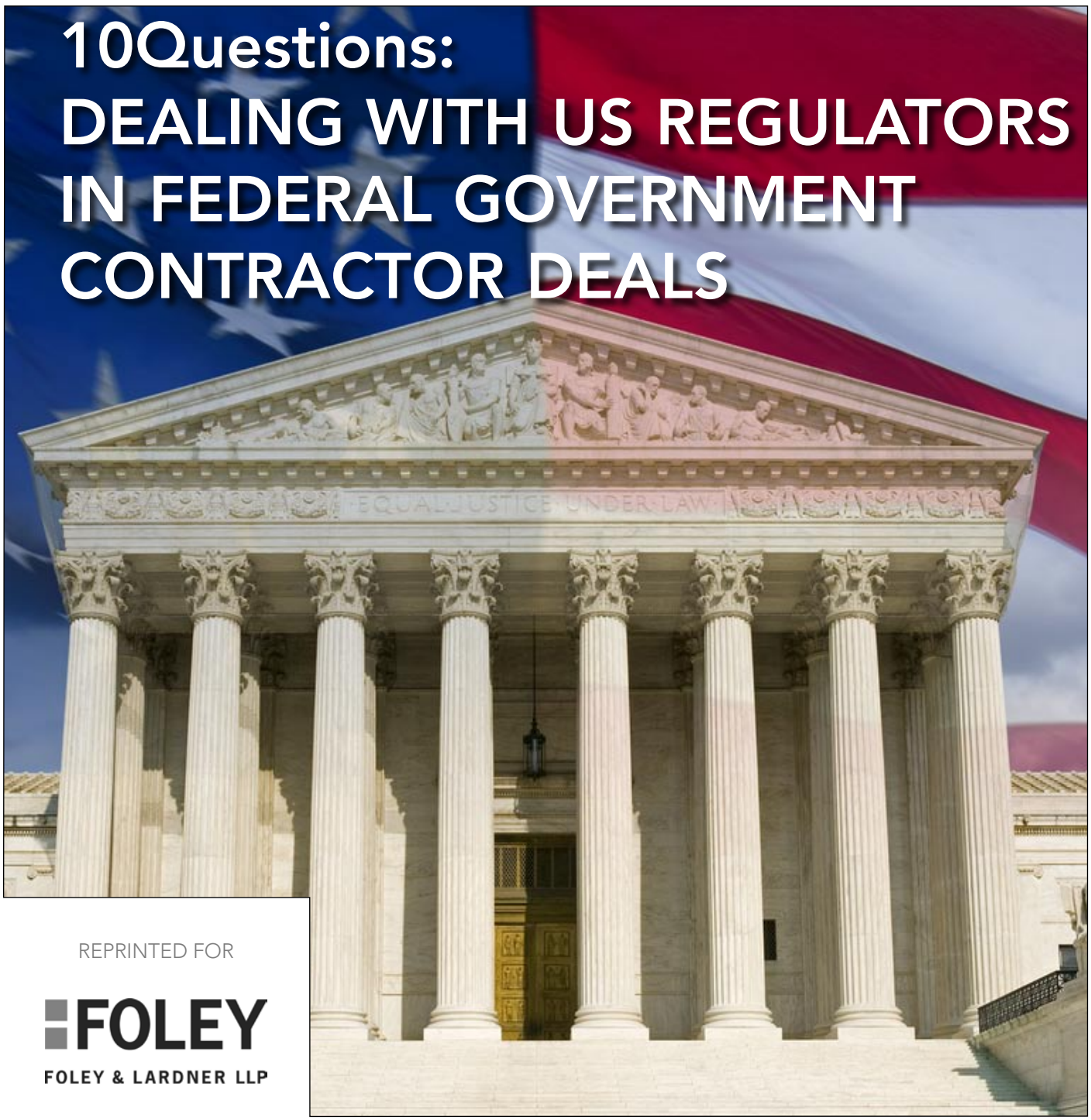
REPRINTED FROM EXCLUSIVE ONLINE CONTENT PUBLISHED IN:
MAY 2012

10Questions: DEALING WITH US REGULATORS IN FEDERAL GOVERNMENT CONTRACTOR DEALS



REPRINTED FOR

FOLEY & LARDNER LLP

FW speaks with David T. Ralston at Foley & Lardner about dealing with US regulators in federal government contractor deals.

David T. Ralston
Partner
Foley & Lardner LLP

David T. Ralston is a partner at the Washington, DC office of Foley & Lardner LLP. His practice focuses on US government contracts, national and homeland security, and rail and air transportation. Mr Ralston has handled virtually all aspects of government contracts, including bid and small business size protests, claims, defective pricing, intellectual property, qui tam litigation, and Cost Accounting Standards matters. He has successfully defended government contractors against fraud and bribery charges and represented firms in debarment/suspension proceedings at numerous federal agencies. Mr Ralston frequently lectures and writes on US and multi-national government procurement matters. He can be contacted at +1 (202) 295 4097 or by email: dralston@foley.com.

FW: Would you provide a general overview of the special regulatory issues that arise when a non-US firm acquires a US government contractor?

Ralston: While most US government contractor acquisitions will raise some regulatory issues and government approval requirements, there are three particularly significant issues that must be addressed when the acquiring firm is not a US company. Each of these arises when the target firm's contracts involve US defence, national or homeland security matters, or the firm exports controlled items. First, a US company must hold a 'facility security clearance' to be 'cleared' to perform US government contracts involving classified information. Should a non-US firm gain control of the cleared firm, the result can be revocation of the clearance and loss of those contracts. To avoid loss of the target firm's clearance, the acquiring firm must implement mitigation steps, possibly including corporate control measures, to avoid any risk that the acquisition could result in unauthorised persons gaining access to classified information, and must obtain government approval of the mitigation plan.

Second, the Export Administration Regulations (EARs) and the International Traffic in Arms Regulations (ITARs) govern, respectively, the export of products, technology and services that have dual civilian-military/strategic application, or are intended for military or military-related use. When the target company has EAR/ITAR-controlled exports, the acquiring firm has to obtain government approval of the transfer of the licenses and take steps to prevent the export of controlled items to unauthorised parties, including the acquiring firm's own employees who are not US citizens. Third, the Committee on Foreign Investment in the United States (CFIUS), an inter-agency, cabinet-level committee, determines whether transfer of control of any US firm to a 'foreign person' presents a threat to US national security – irrespective of whether the target is privately-held, publicly-traded, or a government contractor. While a CFIUS review is triggered by a voluntary request by the parties to the acquisition transaction, when the target firm has a facility security clearance or EAR/ITAR-controlled exports, seeking a CFIUS review will effectively be a requirement and, when there are significant defence, national security or homeland

security contracts at issue, requesting a review is recommended. A non-US acquirer will want to determine at the outset of the negotiation/acquisition process whether those issues will arise because, if they do, they will significantly impact the due diligence process and can impact the structure and pricing of the transaction.

FW: In these types of deals, involving a non-US firm as a buyer, there may be complications associated with gaining access to classified information held by the target company. How are those complications resolved?

Ralston: The US government's system for corporate access to classified information is implemented by the National Industrial Security Program, managed by the Defense Security Service (DSS), a US Department of Defense (DoD) agency. DSS issues the National Industrial Security Program Operating Manual (NISPROM), which provides the requirements to obtain – and maintain – facility and personnel security clearances for contractor access to classified information needed for government contracts. Maintaining a NISPROM facility security clearance in good standing is a prerequisite for continued performance of US government contracts involving classified information. When a cleared firm may fall under "foreign ownership, control or influence" (FOCI), which obviously will occur when a foreign interest acquires ownership of a cleared firm, the parties to the transaction have to undertake NISPROM-required risk-mitigation steps to avoid revocation of a target firm's facility security clearance, and concomitant loss of valuable contracts. NISPROM provides the mitigation plan requirements, but the actual plan approval is managed by the federal agency responsible for the classified information at issue, such as DoD or the Central Intelligence Agency, which is called the Cognizant Security Agency (CSA). NISPROM effectively forces security clearance issues to the forefront in an acquisition, as it requires that firms holding facility security clearances notify their CSA as soon as the cleared firm enters into negotiations for a proposed merger, investment, or similar act, with a foreign interest. Addressing NISPROM concerns also plays into obtaining CFIUS clearance, as NISPROM is a specific CFIUS review matter, and it can be expected that CFIUS will require a NISPROM-approved mitigation plan as a condition of CFIUS clearance.

There are four NISPROM mitigation approaches, depending upon the extent of foreign interest control of the cleared US firm. First, when the non-US firm investment in the cleared firm does not constitute sufficient voting control to be entitled to representation on the cleared firm's corporate board, and the principal corporate officers of the cleared firm are and will remain US citizens, a board resolution and/or bylaws amendment by the cleared firm will suffice. Those documents identify the foreign interest, acknowledge the cleared firm's obligation to continue compliance with NISPROM requirements, and certify that the foreign interest will not have/cannot obtain unauthorised access to classified information. Second, when the foreign interest's investment will result in board representation, but not voting control of the cleared firm, a Security Control Agreement (SCA) is employed. An SCA requires that the cleared firm's security and export control matters be managed through a Government Security Committee comprised of senior management and outside directors who are cleared US citizens, and that the board directors representing the non-US owner investment interest not have access to classified information.

Third, the most stringent approach is a voting trust or proxy agreement, which is employed when the foreign interest will obtain voting control of the cleared firm. Title to the controlling interest in the cleared US firm or its subsidiary is placed in a voting trust, or the investment interest is placed, via a proxy agreement, in the hands of proxies. The trustee or the proxies must be cleared US citizens, and under the respective agreements they possess essentially complete freedom of control from the foreign interest, subject only to the terms of the trust or proxy agreement. NISPROM does permit trust/proxy agreement provisions that require the foreign interest's approval for matters such as sale of the company or substantial assets, pledges, mortgages, mergers, and similar major corporate transactions. Fourth, in lieu of a voting trust or proxy agreement, a Special Security Agreement (SSA) can be proposed when the foreign interest's home country has, at least, a bilateral security agreement with the US.

FW: Another key area for analysis is export controls and sanctions. What assessments need to be carried out concerning licenses and permissions, products and technologies, compliance issues, risk factors, etc.?

Ralston: The EARs, enforced by the Commerce Department's Bureau of Industry and Security (BIS), control the transfer and retransfer of US-origin 'dual-use' products, technology and services – that is,

commercial items with dual use in both commercial, and military and strategic applications. The ITARs, enforced by the State Department's Directorate of Defense Trade Controls (DDTC), control the export of weapons and military technology listed on the US Munitions List. Of the two regulations, the ITARs are the more stringent. In general, both regulations prohibit unlicensed transfer of controlled exports to foreign nationals, and an acquisition by a non-US firm of a government contractor that exports under EAR/ITAR licenses necessitates amendment/transfer of the licenses to reflect the change of control to the acquiring firm. To obtain BIS/DDTC approval will require that the acquiring firm certify continued compliance with EAR/ITAR requirements. I would underscore that simply sharing controlled items – such as technology or data – with an unlicensed foreign national constitutes a 'deemed export', and there is no exception for foreign nationals merely because they are employed by an acquiring firm, or another firm (even corporate affiliates) that may hold an export control license, or because the data sharing occurs in the US. This requires that multi-national firms maintain strict internal export control policies and procedures preventing their own non-US employees from gaining access to controlled items – including technology and data.

In the acquisition context, the target firm must obtain export control licenses for the acquirer's foreign national employees before the target firm may permit the acquirer to have access to EAR/ITAR-covered exports. Similar to NISPROM, under the ITARs an acquisition in which a 'foreign person' gains ownership or control of a firm listed in or exporting ITAR-covered items triggers a 60-day advance notice requirement to DDTC. This provides DDTC an opportunity to object to the transaction, and DDTC can raise the objection at CFIUS. Again, similar to NISPROM, export controls are key points in a CFIUS review and successfully addressing EAR/ITAR matters – through a mitigation plan if necessary – is frequently a prerequisite for CFIUS clearance. Fortunately, there have been several recent developments that may ease the ITAR compliance process, and acquisitions affected by them. In late 2011, DDTC implemented a new ITAR policy to permit transfer of unclassified defence articles to persons with security clearances issued by certain US allies. Also, treaties reached in 2007 between the US and the UK and Australia concerning ITAR matters recently came into force through an ITAR amendment, so that certain UK and Australia companies that obtain pre-approval from DDTC can now be exempted from general ITAR licensing requirements, subject to several limitations.

FW: When a 'non-US' buyer is involved, a government contractor acquisition may be subject to CFIUS review. How does this affect the transaction process?

Ralston: While, as noted, a CFIUS review is voluntary, CFIUS has its ways of prodding a 'voluntary' request when it has concerns about a transaction. Therefore, whether to seek a CFIUS review when the target firm holds defence or national security contracts should be addressed early on in the acquisition transaction. That said, seeking a CFIUS review, even when the target firm holds US government contracts, is not always the right direction. In short, when NISPROM or EAR/ITAR issues are present, requesting a CFIUS review is effectively a necessity; and when the target holds significant government contracts involving DoD, Homeland Security, national security agencies, critical infrastructure or technologies, or military supply chain sensitive materials, even though NISPROM may not be implicated, requesting a CFIUS review is recommended.

On the positive side, a CFIUS review can be a something of a 'safe-harbour', because once the transaction is cleared by CFIUS, the transaction cannot be reviewed again by it on national security grounds absent a showing of material misrepresentation to CFIUS, new legislation, or a breach of a material condition in an agreement with CFIUS. By contrast, without a CFIUS review, the transaction remains open to challenge on national security grounds practically indefinitely.

A CFIUS review is initiated by the parties filing a formal notice with CFIUS, but is often preceded by an informal notice and review process with CFIUS. In the informal process, the parties provide CFIUS with salient details about the transaction and discuss appropriate risk mitigation steps to address obvious national security concerns, such as NISPROM and EAR/ITAR issues. CFIUS may propose additional mitigation steps and, if accepted by the parties, those steps are often memorialised in an agreement with CFIUS. Ideally, the informal process will result in a subsequent 'pre-packaged' formal notice to CFIUS that presents a comprehensive resolution of national security concerns so the transaction is ready for clearance by CFIUS. As to the formal review process, CFIUS has 30 days after notice is filed to conduct its review and decide whether an investigation will be needed. If an investigation is not ordered, the CFIUS review is concluded – which is the expected

outcome when CFIUS concerns have been adequately addressed. If an investigation is ordered, it must be completed within 45 days. Thereafter, the President has 15 days to announce a final decision, which may include no action, blocking the transaction, or if the transaction has already closed, ordering divestiture.

FW: What other regulatory approvals are required in government contractor deals?

Ralston: For acquisitions that are asset sale transactions, government approval will be needed to transfer existing government contracts to the acquiring firm, which is termed a 'novation'. For mergers, consolidation or reorganisations, novations are not required because, in essence, the government contracts continue with the same entity, that is, the target firm.

In substance, a novation is a contract assignment with continued recourse to the assignor in the event the assignee defaults on the contract obligation. Assuming the novation requirements are met, the government routinely approves them. Proposals that the target may have submitted in response to US government solicitations can be transferred as part of the acquisition without formal government approval. Nonetheless, proposals need to be reviewed to address whether the acquisition will impact the offeror's responsibility, financial capability, or other aspects such as key personnel or performance record that may be reflected in the proposals, and consideration should be given to providing the government with notice of the transfer to avoid later bid protest issues directed at the change in offeror.

When small business contracts are at issue, the situation can be complex and require expert attention before the acquisition is consummated so that the parties can evaluate the impact of the acquisition on the small business contracts. In short, current small business contracts generally may continue, but new small business contracts are precluded, and the exercise of contract options on existing small business contracts will not count toward agency small business goals, unless the combined firm – acquired plus target – is within the applicable small business size limit. A similar outcome results for small business firms with Small Business Innovation Research grants: existing grants may continue, but new grants are precluded.

FW: What issues arise when assessing conflicts of interest regarding the target company?

Ralston: During the due diligence process, acquirers of US government contractors always need to assess whether the acquisition will result in Organizational Conflicts of Interest (OCIs) that could result in disqualification from future procurements or create conflicts under existing contracts. A typical OCI example arising in acquisitions is when the target firm has played a role as a key advisor to a government agency on a government procurement in which the acquiring firm is a competitor. The concern is that the target firm, knowing it may be acquired by the acquiring firm, has or will skew its advice to the agency in a manner designed to tilt the procurement in favor of its acquiring firm. Unless addressed, this OCI can – and likely will – result in the acquiring firm being precluded from award of the contract. When OCIs are identified timely, however, mitigation plans can be submitted to the agency, and if approved, the OCI will be waived by the agency. In a similar vein, some government contracts have provisions requiring on-going, or 'evergreen' disclosure of OCIs if learned of during contract performance. An acquisition can trigger those disclosure requirements, which in turn can result in termination of the contract – obviously a bad outcome, particularly if the contract is of significant value. The proper step here is to provide the OCI notice to the agency prior to closing on the acquisition and to obtain a pre-closing waiver.

FW: What kinds of questions need to be answered in relation to the target's compliance program?

Ralston: With few exceptions, firms with a US government contract exceeding $5 million have – or should have – compliance programs addressing government contracts issues. A standard part of the due diligence process is to request a copy of the target firm's compliance program, an interview of the target's compliance officials, and copies of allegations received under the compliance program in the last three years and their ultimate resolution. If the target does not have a program, or resists providing access to compliance officials or materials, those are red flags that should trigger in-depth due diligence inquiry by attorneys familiar with US government contracts. Representations and/or warranties in the transactional documents will likely be needed to address unresolved compliance issues.

FW: Intellectual property can often play a significant role in government contractor deals. Would you explain the issues surrounding the US government's treatment of the contractor's IP, and

the IP aspects of existing agreements?

Ralston: The rules applicable to US government contracts and IP can differ dramatically from the rules applied in the commercial marketplace, and, to some extent, the rules applied outside the US. The rules can also differ depending upon whether the federal agency is military or civilian. With regard to patents, the US government will have a fully-paid up, worldwide license to practice an invention that is first conceived of, or reduced to practice, in the performance of a government contract. If the contractor takes certain notice steps on a timely basis, it can patent and obtain title to such inventions, subject to the government license, which give the contractor the right to commercialise the patented invention. As to patent infringement by government contractors during performance of a government contract, the government is generally financially liable for the infringement, but can look to the contractor for indemnification if an appropriate clause is in the contract. As for trade secrets, which the US government lumps under the general title of 'technical data', the government has three treatment levels. If the trade secret data were developed exclusively with federal funds, or the contractor failed to take required protective steps for the data, the government obtains unlimited rights in the data. Here the government virtually owns the data, and could use it to compete with the contractor in the commercial marketplace.

With trade secret data developed in part with government funds – known as 'mixed' funding – the government expects, at least, what are essentially government purpose rights, although the name may differ depending on the agency involved. As the name suggests, those rights limit the use of the data to government purposes, but government purposes include the right to give the data to another contractor to compete with the original contractor on future government contracts that require use of the data. It does not include, however, the right to give the data to another firm to permit that firm to compete in the commercial, non-US government marketplace. Finally, the government accords the highest level of protection to trade secret data developed exclusively at private expense, which is considered 'limited rights data', although again the precise name may differ depending on the agency. As to data pertinent to non-commercial items, this generally precludes disclosure of the data outside the government without the contractor's written permission. Regarding commercial items, the government will accept the contractor's commercial licensing agreement tailored to reflect certain government requirements.

FW: To what extent do the target's employees and subcontractors need to be carefully vetted? What red flags might be uncovered during the due diligence process?

Ralston: With regard to the target's employees, two key questions arise. First, whether senior corporate and division managers were formerly high-level government officials. If so, then their compliance with the federal rules governing their post-government employment needs to be reviewed with them on an individual basis. Second, the US government just issued a new regulation on personal conflicts of interest directed at contractor personnel who advise a federal agency on what are termed 'inherently governmental functions', such as procurement contracts. The due diligence process should focus on determining that the new regulation has been implemented, and any such personal conflicts identified and resolved. Additionally, the target, the target's management, and major subcontractors need to be checked against the government's Excluded Parties List, which is the list of persons and firms suspended or debarred from government contracting.

FW: Anti-bribery and anti-corruption laws can have a major impact on government contractor deals. What particular aspects of those laws should be considered as to government contractors?

Ralston: Beyond the usual due diligence review of those issues, any of the target's US government contracts performed in Iraq or Afghanistan should be identified and subject to rigorous due diligence review, including interview of corporate personnel with responsibility for those contracts. Simply operating in those theaters raises red flags as to bribery and corruption concerns, as well as to government claims and contract disputes, which abound. Consider also that, going forward, the glide path for US involvement in those theaters is on a decidedly downhill slope. That generally means the upside financial potential for contractors is limited, while the exposure for past contractor misdeeds can be virtually unlimited. Few acquirers relish buying into past misdeeds – particularly when, going forward, the contracting picture is not terribly promising. ■