BRIEFING PAPERS® SECOND SERIES

PRACTICAL TIGHT-KNIT BRIEFINGS INCLUDING ACTION GUIDELINES ON GOVERNMENT CONTRACT TOPICS

Federal Contractor Compliance Developments: Cybersecurity, Labor And Employment, And M&A Transactions

*By Agnes P. Dover, Michael D. McGill, Ogechi C. Achuko, and Michael J. Scheimer**

Doing business with the U.S. Government has long forced companies to understand and comply with a complex, broad web of statutory and regulatory obligations. Over the past several years, performing work for the Government—either directly through a prime contractor or indirectly through a subcontract—has gotten even more complicated. This BRIEFING PAPER focuses on three developments that impose additional requirements or necessitate heightened diligence for companies that perform work for the Government. The first one—proliferation of cybersecurity obligations—is not surprising given recent headlines of significant data breaches. The second one—expansion of labor and employment requirements—is the product of President Obama's administration's increased emphasis on protecting American workers. The third one—the special risks associated with merger and acquisition (M&A) transactions involving federal contractors—is an outgrowth of the exceptional level of transactional activity among companies in the aerospace, defense, and Government services sectors over these past few years. While the various underlying factors that have driven these developments are not necessarily related, the common thread that runs through each of these areas is that they all raise new regulatory risks and compliance obligations. Given the significant enforcement powers of the Government, through contractual, civil fraud, and even criminal actions, the need to be aware of new regulatory requirements is key.

Heightened Cybersecurity Compliance Obligations

Over the past few years, many new regulatory mandates have been imposed for Government contractors that require implementation of systems to prevent and to report data breaches. Particularly significant are a final rule adding new Federal Acquisition Regulation (FAR) provisions on safeguarding of covered contractor information systems[1] and a Department of Defense (DOD) interim rule imposing cybersecurity requirements on its contractors.[2] These new mandates compel contractors to implement significant new systems to remain compliant.

*Agnes P. Dover and Michael D. McGill are partners and Ogechi C. Achuko and Michael J. Scheimer are associates in Hogan Lovells US LLP.

IN THIS ISSUE:

THOMSON REUTERS

The new FAR rule is the latest step in a series of coordinated regulatory actions, including draft White House Office of Management and Budget (OMB) guidance for federal contracting[3] and implementation of cybersecurity requirements, such as those related to controlled unclassified information (CUI).[4] These actions are meant to clarify the application of the Federal Information Security Management Act of 2002,[5] as amended by the Federal Information Security Modernization Act of 2014[6] (collectively, "FISMA"),[7] which is the preeminent legislation in this area. They also further extend the National Institute of Standards and Technology (NIST) information systems security requirements to contractors and, by doing so, create greater consistency in safeguarding practices across agencies. Under FISMA, each agency is responsible for "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or *on behalf of the agency*; and (ii) information systems used or operated by an agency or *by a contractor of an agency* or other organization on behalf of an agency[.]"[8] FISMA specifically requires agencies to "ensure compliance with. . .policies and procedures as may be prescribed by the [OMB] Director" and information security standards promulgated by NIST.[9]

In turn, NIST Special Publications (SPs) contain the baseline security standards that agencies must follow. Systems operated on behalf of the Government (i.e., by a contractor) have generally been required by FISMA to meet NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations,"[10] and to conform to the same information security processes as Government systems. However, for contractors' *internal* systems that incidentally contain Government information, the application of NIST SP 800-53 controls is generally not appropriate. Thus, the recent cybersecurity regulatory actions discussed below, including the new FAR rule and the related DOD rule, are intended to address cybersecurity for Government information on internal contractor systems. The Government's goal appears to be building consistency of cybersecurity protections horizontally (across the Government) as well as vertically (for Government contractors and the Government's supply chain) to better protect Government information and information systems that may contain such information. While that goal is understandable, the practical effect is that contractors must undertake significant steps to implement systems that satisfy the new requirements.

FAR Final Rule On Safeguarding Of Covered Contractor Information Systems

On May 16, 2016, the FAR Council issued a final rule to implement requirements for the "basic safeguarding" of contractor information systems."[11] The final rule, which took effect on June 15, 2016, added a new FAR subpart and contract clause for safeguarding contractor information systems that process, store, or transmit "federal contract information," i.e., information not intended for public release that is provided by or generated for the Government under a Government contract (excluding information provided by the Government to the public or simple transactional information), residing in or transmitting through its information system.[12]

Specifically, new FAR Subpart 4.19, "Basic Safeguarding of Covered Contractor Information Systems," and an accompanying identically titled contract clause at FAR 52.204-21 identify 15 security requirements for safeguarding a covered contractor information system (e.g., host servers, workstations, and routers).[13] Although the FAR Council suggested in commentary that the final rule is intended to address a basic level of safeguarding and does not equate to heightened safeguards applicable to CUI,[14] the 15 require-

Editor: Valerie L. Gross

Briefing Papers® (ISSN 0007-0025) is published monthly, except January (two issues) and copyrighted by Thomson Reuters, 610 Opperman Drive, P.O. Box 64526, St. Paul, MN 55164-0526. Customer Service: (800) 328-4880. Periodical Postage paid at St. Paul, MN. POSTMASTER: Send address changes to Briefing Papers, 610 Opperman Drive, P.O. Box 64526, St. Paul, MN 55164-0526.

ments are pulled verbatim from NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations."[15] As a result, DOD contractors that have already implemented the NIST SP 800-171 security requirements under the Defense FAR Supplement (DFARS) interim rule on cybersecurity safeguarding[16] (discussed below) should be well positioned to comply with the new FAR rule. DOD (and non-DOD) contractors that have not yet implemented the NIST SP 800-171 security requirements (which are categorized by "family") may wish to consider prioritizing the items set forth in the table on the following page to comply with the new requirements.

Importantly, the FAR rule applies to nearly all acquisitions, even those below the simplified acquisition threshold.[17] It applies to commercial item procurements except for procurements of commercial-off-the-shelf (COTS) items.[18] Additionally, the rule applies to any covered contractor information system, i.e., systems that are owned or operated by a contractor that process, store, or transmit "Federal contract information."[19] The requirements also apply to subcontractors at all tiers when the subcontractor may have "Federal contract information."[20] Unlike the DFARS cybersecurity rule, discussed below, this FAR clause does not impose an affirmative compliance certification upon the contractor or a process whereby a company must present its security safeguards for Government review.

DFARS Interim Rule On Network Penetration Reporting & Contracting For Cloud Services

On August 26, 2015, the DOD issued an interim rule on cybersecurity that significantly amended the DFARS to impose heightened cybersecurity requirements on all DOD prime contractors (including small businesses and commercial-item contractors) and subcontractors at all tiers.[21] Citing "urgent and compelling reasons," including the recent high-profile breaches of Government information systems, the DOD made the rule effective immediately upon publication.[22] The DOD did invite the public to submit comments (by November 20, 2015) to be considered in the formation of a final rule.[23]

Congress spotlighted cybersecurity concerns about the defense contractor community in § 941 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013, which directed the DOD to establish procedures to require cleared defense contractors to report information system and network penetrations and to allow DOD personnel access to the system or network to assess the impact of the penetration.[24] The DFARS interim rule, which implements this provision, makes no mention, however, of similar cyber incident reporting procedures for *cleared intelligence contractors* set out in § 325 of the Intelligence Authorization Act for FY 2014.[25] Section 325 instructed the Office of the Director of National Intelligence (DNI) and the Secretary of Defense to coordinate and establish procedures to permit contractors that qualify as both cleared intelligence contractors under § 325 and cleared defense contractors under § 941 of the FY 2013 NDAA to submit a single report that satisfies both intelligence and defense requirements for cyber incidents.[26] Consequently, contractors covered by both the 2015 DFARS interim rule and the Intelligence Authorization Act requirements should expect further guidance on cyber incident reporting. Later, in the FY 2015 NDAA, Congress mandated that the DOD establish procedures requiring an "operationally critical contractor" to report each penetration of its information system or network.[27]

Implementing this mandate, the DOD's August 26, 2015 interim rule specifically requires contractors to "rapidly report" cyber incidents to the DOD.[28] The rule defines "rapid reporting" as within 72 hours of the contractor's discovery of a "cyber incident"[29]—meaning "actions taken through the use of computer networks that result in an *actual or potentially* adverse effect on an information system and/or the information residing therein"[30]—that "affects a covered contractor information system *or* the covered defense information residing therein, *or* that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support."[31] The interim rule also directs contractors to the Defense Industrial Base (DIB) reporting portal at http://dibnet.dod.mil for the required minimum contents of a report.[32]

Requirements & Procedures For Basic Safeguarding Of Covered Contractor Information Systems

FAR 52.204-21(b)(1)	NIST 800-171 Reference	NIST 800-171 Family
(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	3.1.1	Access Control
(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	3.1.2	Access Control
(iii) Verify and control/limit connections to, and use of, external information systems.	3.1.20	Access Control
(iv) Control information posted or processed on publicly accessible information systems.	3.1.22	Access Control
(v) Identify information system users, processes acting on behalf of users, or devices.	3.5.1	Identification and Authentication
(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	3.5.2	Identification and Authentication
(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	3.8.3	Media Protection
(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	3.10.1	Physical Protection
(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.	3.10.3 3.10.4 3.10.5	Physical Protection
(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	3.13.1	System and Communication Protection
(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	3.13.5	System and Communication Protection
(xii) Identify, report, and correct information and information system flaws in a timely manner.	3.14.1	System and Information Integrity
(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.	3.14.3	System and Information Integrity
(xiv) Update malicious code protection mechanisms when new releases are available.	3.14.4	System and Information Integrity
(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	3.14.5	System and Information Integrity

The DOD subsequently issued a revised interim rule on December 30, 2015, giving contractors significantly more time to implement the requirements of NIST SP 800-171.[33] (Although the DOD had issued the now superseded DFARS Class Deviation 2016-0001 on October 8, 2015, allowing an offeror or contractor up to nine months to comply with the multi-factor authentication standards in NIST SP 800-171, that was the only 800-171 standard that the DOD allowed extra time to implement).[34] The second interim rule was published "to provide immediate relief from the requirement to have NIST 800-171 security requirements implemented *at the time of contract award*."[35] Under the rule, contractors are now directed to implement NIST SP 800-171 standards "as soon as practical, but not later than December 31, 2017."[36] Despite the additional time, contractors are still obligated to notify the DOD Chief Information Officer, within 30 days of award, of any NIST SP 800-171 security requirement that has not been implemented at the time of contract award.[37] It appears that, absent such notice, the DOD may presume contractors are meeting *all* of the NIST SP 800-171 security requirements.

Under the earlier version of the interim rule, covered DOD contractors were required to flow down the *substance* of the "Safeguarding Covered Defense Information and Cyber Incident Reporting" clause at DFARS 252.204-7012 to *all* subcontractors.[38] Now, the exact phrasing of the safeguarding clause must be flowed down "without alteration," except as needed to identify the contracting parties subject to the clause, but the flow down of the clause is limited only to subcontracts and "similar contractual instruments" that involve either (a) "operationally critical support" or (b) a covered contractor information system.[39]

Expanded Labor & Employment Compliance Obligations

Contractors and subcontractors generally understand that performing work for the Federal Government means complying with certain heightened labor and employment requirements. The compliance obligations imposed on federal contractors and subcontractors in this area have evolved rapidly over the past several years, driven by Executive Orders,[40] rulemakings, and guidance from President Obama's administration. While most contractors and subcontractors are familiar with the longstanding equal employment opportunity and affirmative action requirements, it is critical to not only meet those standards but to also comply with the bevy of new and amended requirements that were recently adopted or that will take effect in the near future. The following section of this BRIEFING PAPER highlights some of the more significant developments related to the labor and employment requirements that apply to federal contractors and subcontractors.

Contractor Minimum Wage

To implement Executive Order No. 13658, "Establishing a Minimum Wage for Contractors," which was signed by President Obama on February 12, 2014,[41] the Department of Labor (DOL) issued a final rule on October 7, 2014, that raised the minimum wage to $10.10 for workers performing "on" or "in connection with" certain types of federal contracts and "contract-like instruments" resulting from solicitations issued on or after January 1, 2015, or awarded outside the solicitation process on or after January 1, 2015 (e.g., contracts awarded on a sole-source basis).[42] The rule applies to four categories of prime contractual agreements: (1) contracts for construction under the Davis-Bacon Act[43] (DBA) valued at more than $2,000; (2) service contracts under the Service Contract Act[44] (SCA) valued at more than $2,500; (3) concessions contracts; and (4) contracts in connection with federal property or lands and related to offering services for federal employees, their dependents, or the general public (e.g., child care centers, gifts shops, etc. located in federal buildings).[45] The requirements also apply to subcontracts issued under covered prime agreements.[46] The requirements only apply to contracts with the Federal Government requiring performance in whole or in part within the United States; if a contract with the Federal Government is to be performed in part within and in part outside the United States and is otherwise covered by the Executive Order No. 13658 and the DOL rule, the minimum wage requirements only apply to that part of the contract that is performed within the United States.[47]

The minimum wage applies to *all* workers performing on or in connection with a covered contract or subcontract whose wages are governed by the Fair Labor Standards Act[48] (FLSA), SCA, or DBA.[49] Coverage is not limited to direct employees of the prime contractor and subcontractors; it extends to any workers who satisfy this test, including independent contractors and agents.[50] If a worker is entitled to a *higher* wage rate under another federal, state, or local law (including the SCA or DBA), the contractor or subcontractor must pay the worker at the higher wage rate.[51] Workers who are employed in a bona fide executive, administrative, or professional capacity or who otherwise are exempt from the FLSA's minimum wage and overtime requirements are

not entitled to receive this special minimum wage.[52] FLSA-covered workers performing "in connection with" covered contracts are also excluded if they do not perform any direct work "on" the contract and spend less than 20% of their work hours in a particular week performing "in connection with" covered contracts and subcontracts.[53] The onus will be on contractors to accurately apply these thresholds, which will not always be straightforward or easy to track.

The minimum wage rule further imposes the following requirements on covered contractors and subcontractors:

(1) Covered contractors and subcontractors must post a notice summarizing employees' rights under the new regulations;[54]

(2) Covered contractors and subcontractors must pay wages no later than one pay period (which may not be longer than semi-monthly) following the end of the pay period during which the worker earned the wages;[55] and

(3) Covered contractors and subcontractors must maintain records of wage payments for each worker for three years. These records must include the following information for each worker: (a) name, address, and social security number; (b) occupation or classification; (c) rate of wages paid; (d) number of daily and weekly hours worked; (e) deductions made; and (f) total wages paid.[56]

The Secretary of Labor will set the minimum wage annually and publish wage rates at least 90 days prior to the effective date.[57] The current minimum wage can be found on the Wage and Hour Division's website at http://www.dol.gov/whd/ and the Wage Determinations Online website at http://www.wdol.gov. Contractors found noncompliant may be required to pay back wages and be subject to payment withholding, termination, and debarment (i.e., exclusion from award of future federal contracts for a period of time).[58] Contractors should keep in mind, however, that if the minimum wage increases after agreement on price for a particular contract, the contractor may be entitled to an equitable price adjustment to account for an increase in the applicable minimum wage.

To comply with this rule, it is critical for covered contractors and subcontractors, if they have not done so already, to (1) identify any employees covered by the new minimum wage requirement, (2) adjust the wages of employees as necessary, (3) post the required notice concerning employee rights, and (4) adjust recordkeeping policies as necessary.

A subsequently issued interim rule, effective February 13, 2015, implemented Executive Order No. 13658 and the DOL minimum wage final rule for acquisitions subject to the FAR (e.g., not concessions contracts) by creating a new FAR Subpart 22.19 and a new clause at FAR 52.222-55, "Minimum Wages Under Executive Order 13658."[59] The interim rule provides detail and instructions regarding requests for and entitlement to contract and subcontract price adjustments resulting from the annual minimum wage increases required by Executive Order No. 13658.[60]

Prohibiting Discrimination On the Basis Of Sexual Orientation & Gender Identity

Another DOL rule that took effect in 2015 prohibits federal contractors from discriminating in employment on the basis of "sexual orientation" or "gender identity" in addition to the existing protected categories.[61] This final rule issued by the DOL's Office of Federal Contract Compliance Programs (OFCCP) implements Executive Order No. 13672, signed by President Obama on July 21, 2014,[62] which amended Executive Order No. 11246[63] that previously only prohibited discrimination by federal contractors and subcontractors on the bases of race, color, religion, sex, and national origin and required them to take affirmative measures to prevent discrimination on those bases from occurring. The final rule revised the DOL regulations effective April 8, 2015, by substituting the phrase "sex, sexual orientation, gender identity, or national origin" wherever the phrase "sex or national origin" previously appeared in the regulations implementing Executive Order No. 11246.[64] Under the revised regulations, contractors and subcontractors must (1) update the Equal Employment Opportunity (EEO) clause in new and modified subcontracts to reference sexual orientation and gender identity, (2) include language in job advertisements stating that all applicants will be considered without regard to sexual orientation or gender identity, and (3) post new workplace notices that include references to sexual orientation and gender identity.[65]

Given the expansion of protection to the classifications of "sexual orientation" or "gender identity," it is important to understand what the rule does *not* require, as the requirements are not exactly the same as they are for other protected classifications. The rule does *not* mandate that contractors (a) collect any information about the sexual orientation or gender identity of applicants and employees, (b) request that employees voluntarily self-identify as having a particular sexual orientation or gender identity, (c) conduct any compensation, hiring, or other statistical data analysis with

respect to sexual orientation or gender identity, or (d) set placement goals on the basis of sexual orientation or gender identity.[66] Although the rule does not prohibit contractors from asking applicants and employees to voluntarily provide this information, doing so may be prohibited by state or local law and should be viewed cautiously.

To comply with this rule, contractors and subcontractors, if they have not done so already, will need to (1) update their EEO policy statements and internal handbooks and other documentation to include sexual orientation and gender identity, (2) update subcontract flowdown clauses to include the new requirements, (3) include the expanded nondiscrimination statement in job advertisements, (4) post the required workplace notices, and (5) add these categories to equal employment training.

An interim rule effective April 10, 2015,[67] subsequently adopted as final without change,[68] amended the FAR to implement Executive Order No. 13672, as well as the DOL final rule. As amended, the FAR implements Executive Order No. 11246 in FAR Subpart 22.8, "Equal Employment Opportunity," the clause at FAR 52.222-26, "Equal Opportunity," and in related clauses.

Sex Discrimination Guidelines For Federal Contractors

On June 15, 2016, the DOL issued a final rule updating the OFCCP Sex Discrimination Guidelines, which had not been updated since the 1970s, despite drastic changes in the law.[69] The rule replaced outdated guidance with the OFCCP's recent interpretations of Executive Order No. 11246, "Equal Employment Opportunity," as amended,[70] and the OFCCP's and the Equal Employment Opportunity Commission's (EEOC) recent interpretations of Title VII of the Civil Rights Act of 1964.[71]

The rule, which took effect on August 15, 2016, applies to employers with federal contracts or subcontracts totaling $10,000 or more, unless otherwise exempt.[72] The rule applies to all employees who work for a covered employer.[73] As such, the rule's application is not limited to employees who work on a federal contract.

The rule is comprehensive, covering many topics related to sex discrimination, including the following:

(1) *Transgender Employees*—The rule provides that discrimination on the basis of an employee's gender identity or transgender identity is unlawful sex discrimination.[74] Additionally, it prohibits contractors from denying transgender employees access to use bathrooms, changing rooms, showers, and similar facilities consistent with the gender with which they identify.[75] The preamble of the rule also notes that a contractor's categorical exclusion of medical coverage for care related to gender transition or gender dysphoria may constitute unlawful sex discrimination if it singles out services on the basis of gender identity or transgender status.[76]

(2) *Pregnancy Discrimination/Accommodations*—The rule goes beyond the traditional requirement that contractors must treat women affected by pregnancy, childbirth, or related medical conditions at least as well as others for all employment-related purposes, including fringe benefit programs.[77] Additionally, the rule provides a nonexhaustive list of "related medical conditions," including, lactation, gestational diabetes, and other after-effects of delivery.[78] Contractors must generally provide workplace accommodations to an employee who needs such accommodations due to pregnancy, childbirth, or related medical conditions, particularly if the employer grants similar accommodations to other employees who are unable to perform their regular job duties because of work injuries or disabilities.[79] The rule provides practical examples of leave policies and reasonable accommodations to address pregnancy bias, childbirth, and related medical conditions, including extra bathroom breaks, adequate time and place for breastfeeding, and light-duty or modified job assignments.[80]

(3) *Sex Stereotyping*—Contractors are prohibited from treating employees and applicants adversely because they do not fit gender norms, including in regard to looks, demeanor, and skills.[81] The rule highlights examples of unlawful sex stereotyping of both men and women. For example, a contractor may not deny fathers flexible workplace arrangements that would be available to mothers solely based on gender stereotypes about childcare responsibilities.[82] Other forms of unlawful sex stereotyping include failing to promote a woman because she does not wear high heels and make up and harassing a male because he is considered effeminate.[83]

(4) *Compensation Disparities*—Contractors are prohibited from compensating workers differently—in wages, fringe benefits, and earnings opportunities—because of their sex.[84] The rule bans sex discriminatory compensation both on an individual and systematic basis.[85] Discriminatory practices include contractors denying women equal opportunities for overtime hours, commissions, and trainings

that may lead to advancement to higher paying positions.[86] The rule specifically lists certain types of fringe benefits, such as medical, hospital, accident, life insurance, and retirement benefits, profit-sharing and bonus plans, leave, and other privileges of employment.[87] The rule requires contractors to provide male and female employees equal benefits when participating in fringe benefit plans, even if the contractor must incur greater expenses by doing so.[88]

(5) *Intersection With Affirmative Action Requirements*—The rule states that "under no circumstances will a contractor's good faith efforts to comply with the affirmative action requirements" under the OFCCP's preexisting regulations be considered a violation of the rule.[89] The OFCCP notes that the rule should not deter contractors from targeted efforts to recruit and advance women in order to comply with their affirmative-action obligations.[90]

The rule includes an appendix that contains "best practices" for keeping workplaces free of unlawful sex discrimination. Best practices listed include, for example, designating single-user restrooms and showers as sex-neutral, providing appropriate flexible workplace policies, and providing anti-harassment training to all personnel.[91] The rule specifies that these best practices are for contractors' consideration and are not required.[92]

Ban On Pay Secrecy

On September 2015, the DOL issued a final rule, effective January 11, 2016, prohibiting federal contractors and subcontractors from discharging or otherwise discriminating against employees and job applicants for inquiring about, discussing, and/or disclosing their compensation or the compensation of another employee or applicant, subject to certain limited defenses.[93] This final rule implements Executive Order No. 13655, "Non-Retaliation for Disclosure of Compensation Information," signed by the President on April 8, 2014.[94] The rule, which applies to contractors with covered federal contracts and subcontractors valued at more than $10,000 entered into after the rule took effect, bans policies, practices, or rules that prohibit or tend to prohibit employees and applicants from discussing or disclosing compensation.[95] "Compensation" is broadly defined to include "salary, wages, overtime pay, shift differentials, bonuses, commissions, stock options, insurance and other benefits, vacation pay, profit sharing and retirement benefits."[96]

To comply, contractors must incorporate the new nondiscrimination provision into their employee personnel policies, post the nondiscrimination provision electronically or physically in conspicuous places available to employees and job applicants, and review their policies and practices to remove any restrictions on disclosing compensation information that is protected.[97] Notably, the rule does not mandate that contractors provide compensation data on one employee to another or permit employees to obtain unauthorized access to compensation data. Contractors also should be aware that preexisting rules require that they review their compensation practices for any pay disparities and make adjustments as needed.[98]

Paid Sick Leave Rule

On September 7, 2015, President Obama issued Executive Order No. 13706, requiring Federal Government contractors to provide employees with paid "sick leave."[99] On February 25, 2016, the Department of Labor issued a notice of proposed rulemaking, implementing the President's order.[100] The proposed rule "defines terms used in the regulatory text, describes the categories of contracts and employees the Executive Order covers and excludes from coverage, sets forth requirements and restrictions governing the accrual and use of paid sick leave, and prohibits interference with or discrimination for the exercise of rights under the Executive Order."[101] Specifically, the proposed rule requires contractors to provide workers with up to seven days of paid sick leave per year.[102] The proposed rule is prescriptive, requiring contractors to let employees accrue a minimum of one hour of paid sick leave for every 30 hours worked, specifying a wide variety of reasons an employee can use to claim sick leave, and limiting an employer's ability to cap accrued leave to no less than 56 hours a year.[103]

The new paid leave rules will take effect only with respect to new contracts solicited or entered into after January 1, 2017.[104] However, given the nature of the changes, contractors would be well advised to begin preparing to implement the new policies as soon as possible. Contractors may wish to consider, among other steps, preparing to update their employee policies and to modify their benefits systems consistent with the accrual of sick leave and other mandatory terms.

Use Of Background Checks

In addition to the rulemakings, the OFCCP issued Directive 2013-02 establishing its enforcement position on employer use of criminal background checks.[105] The OFCCP has adopted the EEOC's position on employer use of criminal record information to screen applicants. According to

the OFCCP, taking adverse employment action (e.g., refusing to hire) based on criminal record information can constitute discrimination on the basis of race or national origin.[106] In particular, the OFCCP is likely to find discriminatory a policy of *per se* exclusions due to criminal record information or an employer's policy of asking employees about criminal record information on job applications. The OFCCP asserts that employers should conduct an individualized assessment of whether criminal conduct warrants an adverse hiring or other employment decision, such as by considering the nature and gravity of the offense, the time that has passed since the offense, and the nature of the job held or sought.[107]

For most contractors, the following "best practices," set forth in the OFCCP's directive, may be instructive: (1) eliminating any *per se* exclusion policies and instead conducting an individualized assessment of whether criminal conduct warrants an adverse hiring or other employment decision; (2) refraining from inquiring about criminal conduct on job applications and limiting any inquiries about criminal conduct to information that is job-related for the position in question and consistent with business necessity; and (3) keeping all information about an applicant's or employee's criminal records confidential.[108] Contractors also should be mindful to comply with all state or local laws, including "ban-the-box" laws (which prohibit asking about certain criminal conduct on a job application).[109]

Fair Pay & Safe Workplaces

Perhaps the rulemaking that has garnered the most attention in this space is the implementation of Executive Order No. 13673 intended to promote "fair pay and safe workplaces," which President Obama issued on July 31, 2014.[110] On August 25, 2016, the FAR Council issued a final rule implementing Executive Order No. 13673,[111] and the DOL simultaneously issued extensive, final guidance to assist federal agencies in implementing the Executive Order in conjunction with the final FAR rule.[112]

The long-awaited FAR regulations, which take effect October 25, 2016, and will be codified in a new FAR Subpart 22.20, "Fair Pay and Safe Workplaces," will impose a variety of new labor compliance requirements on federal contractors and subcontractors. As part of a phased-in implementation, the disclosure requirements will only apply to prime contractors bidding for new solicitations valued at $50 million or more starting on the effective date. After April 24, 2017, the requirements will apply to solicitations valued at $500,000 or more. Starting October 25, 2017, the requirements will apply to subcontractors, except those supplying strictly commercially-available off-the-shelf ("COTS") items.[113]

Contractors and subcontractors will be required to disclose all violations of certain labor laws that have occurred in the preceding three years.[114] The relevant labor laws include the FLSA,[115] the Occupational Safety and Health Act of 1970 (OSHA),[116] the Migrant and Seasonal Agricultural Worker Protection Act,[117] the National Labor Relations Act (NLRA),[118] the DBA,[119] the SCA,[120] Executive Order No. 11246,[121] Executive Order No. 13658[122] (discussed above), § 503 of the Rehabilitation Act of 1973,[123] the Vietnam Era Veterans' Readjustment Assistance Act,[124] the Family and Medical Leave Act (FMLA),[125] Title VII of the Civil Rights Act of 1964,[126] the Americans With Disabilities Act of 1990,[127] the Age Discrimination in Employment Act of 1967,[128] and equivalent state laws, as defined in guidance issued by the DOL.[129] Importantly, contractors must disclose violations of these laws whether or not the underlying conduct occurred in connection with the award or performance of a Government contract or subcontract.[130]

A prospective contractor will be required to make its initial representation about violations of labor laws upon proposal submission through the System for Award Management. A prospective contractor subject to a responsibility determination will be required to provide details concerning any covered labor violations.[131] Following award, contractors will be required to update their disclosures every six months.[132] The rule provides that the legal entity listed on the bid/proposal or contract (the contractor or prospective contractor) is required to report only its labor violations and not violations of any parent or affiliate.[133] Additionally, a contractor or prospective contractor reporting labor violations will have the opportunity to provide the Contracting Officer with mitigating factors, including steps taken to correct violations and plans to improve compliance.[134]

Agencies will be required to consider these disclosures when determining whether a prospective contractor is presently responsible to receive future federal contracts or, in the case of a postaward disclosure by the contractor, whether the contractor is presently responsible to continue to perform in light of the disclosure.[135] The rule also makes clear that, absent unusual circumstances, a single labor law violation will generally not give rise to a nonresponsibility determination.[136] However, contractors that have been found

to have an unsatisfactory record of labor violations may be required to negotiate and enter into a labor compliance agreement in order to be found "responsible" either before or after award by a federal agency.[137] Additionally, such contractors will potentially be exposed to additional repercussions, including contract terminations for default or cause, referral to an enforcement agency for investigation, and referral for suspension or debarment proceedings.[138]

Starting September 12, 2016, the DOL will begin to offer a "preassessment process" under which current and prospective contractors will be able to voluntarily receive an assessment of their labor compliance history and discuss if additional compliance measures are warranted.[139]

Finally, also as part of the new Fair Pay and Safe Workplaces rulemaking, beginning January 1, 2017, a new clause, "Paycheck Transparency," prescribed for contracts valued over $500,000 will require contractors to provide wage statements to employees performing work under a covered contract subject to the wage records requirements under the FLSA, DBA, and SCA.[140] These statements must include the total hours worked in the pay period, the number of those hours that were overtime hours, the rate of pay, the gross pay, and itemized additions made to or deductions.[141] Also, the contractor must provide written notice of a covered worker's status an independent contractor or employee.[142]

Recent Developments Relevant To M&A Transactions Involving Government Contractors

Last year, 2015, was a record year for merger and acquisition (M&A) activity in the aerospace and defense sector. Forty-three transactions worth more than $50 million were reported with a total deal value of $62 billion, compared to 54 such deals in 2014 with a total deal value of only $24 billion.[143] With the M&A trend continuing, particularly at high-dollar valuations, it is ever important for contractors to make sure that they take reasonable precautions so as not to jeopardize existing and anticipated Government business. Several recent bid protest decisions provide cautionary tales about the implications for failing to do so.

For contracts already in place, there are established processes, set forth in FAR Subpart 42.12, "Novation and Change-of-Name Agreements," for seeking consent through a novation when an assignment of contracts is contemplated or for seeking a change of name agreement if that is planned as part of a transaction.[144] The applicable regulations specifically note that novations are not required in the context of stock purchases so long as there is no change in the nature of the contracting entity.[145] However, there is no established regulatory process under the FAR for assigning proposals or seeking Government recognition that a company's proposal is still valid even when the company or its ownership may have changed. This regulatory gap has given rise to frequent bid protest challenges.

In many cases, the protest grounds revolve around proposals in which a company claimed reliance on its parent's (or other affiliates') resources. Some companies learn the hard way that their competitive position and standing to protest might be affected when they rely on the experience, resources, or past performance of an affiliate that will no longer be affiliated upon consummation of a pending sale and do not take steps to address the potential impact.

Most recently, in *Universal Protection Service, LP v. United States*,[146] the U.S. Court of Federal Claims dismissed a protest on the ground that the protester was not a complete successor in interest to ABM Security Services, the entity that had submitted the proposal to the U.S. Postal Service. The original award decision occurred in January 2015 and was followed by a series of protests and resulting corrective actions. In the meantime, Universal Protection Service purchased ABM Security Services, apparently as part of an asset purchase, and in November 2015, it filed a protest challenging the award to Command Security Group. The Government and intervenor moved to dismiss the protest on the grounds that Universal did not submit a proposal and was not an interested party. In its original proposal in 2014, ABM Security Services had referenced the personnel and back-up support of its parent at the time, ABM Industries, and promised to leverage the ABM network of corporate resources to perform the contract's scope of work. Because Universal did not purchase those other resources, the court concluded that Universal was not in the same position that ABM Security Services was when it submitted the proposal and therefore was not a successor in interest to ABM's proposal and did not have standing to intervene. The court's holding also means that Universal would not have been eligible to receive the award.

In a similar case, *FCi Federal Inc.*,[147] the Government Accountability Office (GAO) sustained a protest challenging award to a company that had been acquired by another company while a proposal the acquired company submitted to the U.S. Citizenship and Immigration Services was pending. The awardee, PAE Professional Services Inc.

(formerly U.S. Investigative Services), had referred to the financial resources and back-office support of its then parent, USIS. By the time of the award, PAE Shield Acquisition Company had purchased USIS in a stock transaction. The GAO found that the original USIS proposal relied, in material respects, on the resources and support of its former parent for management capability, corporate resources, corporate experience, past performance, and financial resources. The GAO concluded that, inasmuch as the offeror was no longer affiliated with USIS, its original proposal was "outdated" and could not form the basis for an award. The GAO, therefore, recommended that the agency reopen discussions with all offerors, request revised proposals, undertake a new evaluation of the revised proposals, and make a new award decision.

Similarly, when a bidder signals, in the middle of a competitive procurement, that it intends to undergo a corporate reorganization and perform the contract in a way that is materially different than described in its proposal, it also risks creating issues for the procuring agency, unless the agency is able to, and does, evaluate the proposal based on the information related to the reorganization. This is illustrated in *Wyle Laboratories, Inc.*[148] and *National Aeronautics and Space Administration—Reconsideration*.[149] Those GAO decisions involved the highly public reorganization of SAIC into two entities, SAIC and Leidos. After SAIC submitted a proposal for medical, biomedical, and health services in support of NASA's human spaceflight programs, it advised NASA that it intended to divest the technical services subsidiary that it originally proposed to perform the requested services. NASA awarded the contract to SAIC, and Wyle Laboratories protested. The GAO concluded that NASA's award to SAIC was improper, because SAIC's intended plan for performing the contract was materially different from the approach NASA evaluated, even though NASA knew that was the case. Of particular significance was that the contract was a cost-reimbursement contract and NASA's cost evaluation was based on performance by a different entity, i.e., the "old" SAIC as it existed before the corporate reorganization separating the company (into "new" SAIC and Leidos).

In subsequent decisions related to awards to SAIC during this reorganization, the GAO noted that its decisions regarding changes in corporate status and restructuring are highly fact-specific and depend "largely on the individual circumstances of the proposed transaction and timing."[150] These decisions suggest that the GAO will expect an agency to evaluate the potential implications of business transactions only where the agency has concrete information, based on the offeror's own proposal or on an intervening consummation of a transaction, indicating that the transaction will materially change, or has materially changed, the proposal such that the offeror does not intend to perform, or will not be able to perform, as proposed.

In *VSE Corp. —Costs*,[151] SAIC had issued a press release stating that it "expected" to split into two companies before contract award. The agency acknowledged that it had not considered the restructuring and contended that it was not required to, stressing that "the restructuring would not occur, if it occurred at all, until after award," and that the effect on SAIC's proposal was "no more than speculation." The agency viewed issues related to changes resulting from the restructuring as matters of contract administration. The GAO agreed, holding that because SAIC did not mention the restructuring in its proposal and the restructuring had not yet occurred, the agency was not required to evaluate it.

Similarly, in *IBM US Federal, a division of IBM Corp.*,[152] the GAO found that where an agency knows that an offeror plans to undergo a corporate restructuring that will involve reallocating resources and experience among companies, it is reasonable for the agency to evaluate the past performance of the entity that submitted the proposal. The GAO concluded there was no evidence that the restructuring of SAIC would have any effect on the performance of the contract and no basis for the protester to complain about SAIC's plan to subcontract all or a large portion of the contract requirements to a newly formed entity spun off from the awardee.

The GAO also has applied this reasoning to other corporate reorganizations. In *Dell Services Federal Government, Inc.*,[153] the GAO denied another protest alleging that an agency improperly failed to consider an anticipated corporate restructuring. There, roughly a year before award, awardee Hewlett Packard's parent company announced that it intended to split into two companies. The GAO held that the procuring agency was not required to consider the restructuring in its evaluation because there was no indication that it would affect the performance of the contract. The GAO found, for example, that the awardee's proposal did not suggest that the awardee would rely upon the resources of its parent company and, even if it did, the agency would not necessarily be obligated to determine whether the split of the parent company would affect the availability of those resources. The agency could assume, unless shown otherwise, that the proposed resources would still be available.[154]

Most recently, in *Veterans Evaluation Services, Inc.*,[155]

the GAO considered whether the Department of Veterans Affairs acted reasonably in not considering the impact of Lockheed Martin's plan to spin-off its Information Systems and Global Solutions business and combine it with Leidos on a proposal submitted by QTC Medical Services, Inc., a Lockheed Martin entity that would move to Leidos in the reorganization. The GAO rejected the protester's argument that the agency failed to consider whether the Lockheed Martin-Leidos transaction would have an impact on QTC. The protester contended that the agency should have evaluated whether Lockheed Martin resources on which QTC indicated it would rely would be available if the transaction closed. The GAO denied these allegations, finding no basis to object to the agency's evaluation.[156]

One of the lessons from these decisions that buyers purchasing a Government contractor entity or related assets should consider is that buyers risk losing contract awards based on proposals that refer to resources of an affiliated entity if those resources are not transferred in the purchase agreement, the companies are no longer affiliated, and there is no agreement in place to secure those resources from the then nonaffiliated entity or elsewhere. Proactive planning in cases involving corporate transactions that occur while important proposals are pending is therefore critical. There may not always be an opportunity to update proposals submitted before a contemplated transaction, but if there is, that could be an appropriate vehicle for addressing the issue—by, for example, describing the anticipated impact of the reorganization on the performance of the contract so that the agency can consider that information in its evaluation.

Additionally, buyers of companies that are in the middle of a competitive process may be able to foresee protest vulnerabilities by examining proposal information during the due diligence process to determine whether the target is relying on the seller's resources for contract performance. To the extent that a prospective buyer is not able to access pending proposals pre-closing, it may wish to seek a representation in the purchase agreement that pending proposals do not rely on resources of a parent or affiliate entity that is not included in the acquisition or take steps to make sure that resources will remain available.

Guidelines

These *Guidelines* are intended to assist you in understanding recent developments affecting Federal Government contractors' compliance obligations regarding cybersecurity, labor and employment, and M&A transactions. They are not, however, a substitute for professional representation in any specific situation.

1. Remember that a FAR rule effective June 15, 2016, "Basic Safeguarding of Covered Contractor Information Systems," sets out heightened cybersecurity requirements for contractors that are based on existing NIST publications. As a result, contractors must comply with 15 security requirements for safeguarding covered contractor information system.

2. Be aware that DOD contractors must also comply with an interim DOD rule effective August 26, 2015, requiring reporting of cyber incidents within 72 hours of discovery.

3. Recognize that under DOL requirements that took effect January 1, 2015, contractors working under certain covered contracts, including construction, service, and concessions contracts, must pay workers a $10.10 minimum wage and maintain records of wage payments.

4. Keep in mind that contractors must also comply with a rule providing paid sick leave for employees that requires accrual of one hour of sick leave for every 30 hours worked.

5. Take steps to ensure that any labor law violations are tracked and reported, as required, under the new Fair Pay and Safe Workplaces regulations.

6. Be aware that contractors that submit proposals while a sale of the company is pending should be cautious about referring to their corporate parents' resources or capabilities.

7. Remember that companies purchasing Government contractor entities should consider potential business impacts relating to proposals that are pending at the time of an acquisition.

ENDNOTES:

[1]81 Fed. Reg. 30,439 (May 16, 2016) (adding FAR subpt. 4.19 and FAR 52.204-21); see 58 GC ¶ 190.

[2]80 Fed. Reg. 51,739 (Aug. 26, 2015).

[3]See https://policy.cio.gov/.

[4]See 81 Fed. Reg. 30,439, 30,440 (May 16, 2016). See generally Vernick & Scheimer, "Feature Comment: Cybersecurity Developments in 2015," 58 GC ¶ 34 (Feb. 3, 2016); 58 GC ¶ 190.

[5]E-Government Act of 2002, Pub. L. No. 107-347, tit. III, 116 Stat 2899, 2946 (2002).

[6]Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014).

[7]Codified at 44 U.S.C.A. §§ 3551–3558.

[8]44 U.S.C.A. § 3544(a)(1)(A)(i)–(ii) (emphasis added).

[9]44 U.S.C.A. § 3544(b)(2)(D)(ii).

[10]Available at http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[11]81 Fed. Reg. 30,439 (May 16, 2016).

[12]"Federal contract information" is specifically defined as "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as that on public Web sites) or simple transactional information, such as that necessary to process payments." FAR 4.1901, 52.204-21(a).

[13]FAR 52.204-21(b).

[14]81 Fed. Reg. 30,439, 30,440 (May 16, 2016).

[15]Available at http://dx.doi.org/10.6028/NIST.SP.800-171. While there has long been guidance (under FISMA) for the protection of unclassified information within federal information systems (i.e., an information system used or operated by an agency, by a contractor of an agency, or by another organization on behalf of an agency), NIST 800-171 was published as additional guidance to protect CUI in nonfederal systems—that is, contractor internal systems that process CUI incidental to developing a product or service for the Government.

[16]See 80 Fed. Reg. 51,739 (Aug. 26, 2015); 80 Fed. Reg. 81,472 (Dec. 30, 2015).

[17]FAR 4.1902, 1903.

[18]FAR 12.301(d)(3).

[19]FAR 4.1901, 52.204-21(a).

[20]FAR 4.1903, 52.204-21(c).

[21]80 Fed. Reg. 51,739 (Aug. 26, 2015).

[22]80 Fed. Reg. 51,739, 51,741 (Aug. 26, 2015).

[23]80 Fed. Reg. 63,928 (Oct. 22, 2015) (extending public comment period from October 26, 2015 to November 20, 2015).

[24]National Defense Authorization Act for Fiscal Year 2013, Pub. L. No. 112-239, § 941, 126 Stat. 1632, 1889 (2013).

[25]Intelligence Authorization Act for Fiscal Year 2014, Pub. L. No. 113-126, § 325, 128 Stat. 1390, 1402 (2014).

[26]Intelligence Authorization Act for Fiscal Year 2014, Pub. L. No. 113-126, § 325(e), 128 Stat. 1390, 1404 (2014).

[27]National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, § 1632, 128 Stat. 3292, 3638 (2014).

[28]DFARS 252.204-7012(c).

[29]DFARS 204.7301.

[30]DFARS 202.101 (emphasis added).

[31]DFARS 252.204-7012(c) (emphasis added).

[32]DFARS 252.204-7012(c)(2).

[33]80 Fed. Reg. 81,472 (Dec. 30, 2015).

[34]Available at http://www.acq.osd.mil/dpap/policy/policyvault/USA005505-15-DPAP.pdf.

[35]80 Fed. Reg. 81,472, 81,473 (Dec. 30, 2015) (emphasis added).

[36]DFARS 252.204-7012(b)(1)(ii)(A).

[37]DFARS 252.204-7012(b)(1)(ii)(A).

[38]80 Fed. Reg. 51,739, 51,747 (Aug. 26, 2015).

[39]DFARS 252.204-7012(m)(1).

[40]See "Non-Retaliation for Disclosure of Compensation Information," Exec. Order No. 13665 (Apr. 8, 2014), 79 Fed. Reg. 20,749 (Apr. 11, 2014); "Further Amendments to Executive Order 11478, Equal Employment Opportunity in the Federal Government, and Executive Order 11246," Exec. Order No. 13672 (July 21, 2014), 79 Fed. Reg. 42,971 (July 23, 2014); "Fair Pay and Safe Workplaces," Exec. Order No. 13673 (July 31, 2014), 79 Fed. Reg. 45,309 (Aug. 5, 2014); "Establishing a Minimum Wage for Contractors," Exec. Order No. 13658 (Feb. 12, 2014), 79 Fed. Reg. 9851 (Feb. 20, 2014); "Establishing Paid Sick Leave for Federal Contractors," Exec. Order No. 13706 (Sept. 7, 2015), 80 Fed. Reg. 54,697 (Sept. 10, 2015).

[41]Exec. Order No. 13658 (Feb. 12, 2014), 79 Fed. Reg. 9851 (Feb. 20, 2014).

[42]79 Fed. Reg. 60,634 (Oct. 7, 2014) (codified at 29 C.F.R. pt. 10); see 56 GC ¶ 329.

[43]40 U.S.C.A. §§ 3141–3148.

[44]41 U.S.C.A. §§ 6701–6707. See generally Donohue & Goddard, "Complying With the Service Contract Act," Briefing Papers No. 01-9 (Aug. 2001).

[45]29 C.F.R. § 10.3.

[46]79 Fed. Reg. 60,634, 60,657–58 (Oct. 7, 2014); 29 C.F.R. § 10.1; see also 29 C.F.R. § 10.2 (definitions of "contract" and "contractor").

[47]29 C.F.R. § 10.3(c).

[48]29 U.S.C.A. § 201 et seq.

[49]29 C.F.R. § 10.3(a)(2).

[50]See 29 C.F.R. § 10.2 (definition of "worker").

[51]29 C.F.R. §§ 10.1(b)(2), 10.5(c), 10.22(a).

[52]29 C.F.R. §§ 10.2 (definition of "worker"), 10.4(e)(3)

[53]29 C.F.R. § 10.4(f).

[54]29 C.F.R. § 10.29. The notice is available through the DOL's website at: https://www.dol.gov/whd/regs/compliance/posters/mw-contractors.pdf.

[55]29 C.F.R. § 10.25.

[56]29 C.F.R. § 10.26.

[57]29 C.F.R. §§ 10.5, 10.12.

[58]29 C.F.R. §§ 10.11(c), 10.44(a), (c), 10.52 & 29 C.F.R. pt. 10 app. A (contract clause), para. (d).

[59]79 Fed. Reg. 74,544 (Dec. 15, 2014).

[60]FAR 52.222-55(b)(3).

[61]79 Fed. Reg. 72,985 (Dec. 9, 2014) (codified at 41 C.F.R. Pts. 60-1,-2,-4, and -50); see 56 GC ¶ 402.

[62]"Further Amendments to Executive Order 11478, Equal Employment Opportunity in the Federal Government, and Executive Order 11246," Exec. Order No. 13672 (July 21, 2014), 79 Fed. Reg. 42,971 (July 23, 2014); see 56 GC ¶ 246.

[63]Exec. Order No. 11246 (Sept. 24, 1965), 30 Fed. Reg. 12,319 (Sept. 28, 1965).

[64]79 Fed. Reg. 72,985 (Dec. 9, 2014) (codified at 41 C.F.R. Pts. 60-1,-2,-4, and -50); see 56 GC ¶ 402.

[65]79 Fed. Reg. 72,985, 72,986 (Dec. 9, 2014). The new rule provides revised language for the "Equal Employment Opportunity Is the Law" notice. 41 C.F.R. § 60-1.42. The DOL issued an "EEO is the Law" Poster Supplement available at https://www.dol.gov/ofccp/regs/compliance/posters/pdf/OFCCP_EEO_Supplement_Final_JRF_QA_508c.pdf. Contracts will not be modified for the sole purpose of adding this requirement, but contracts that otherwise are modified in the ordinary course will also be modified to include these requirements.

[66]79 Fed. Reg. 72,985, 72,986 (Dec. 9, 2014).

[67]80 Fed. Reg. 19504 (Apr. 10, 2015).

[68]80 Fed. Reg. 75,907 (Dec. 4, 2015).

[69]81 Fed. Reg. 39,108 (June 15, 2016) (codified at 41 C.F.R. pt. 60-20); see 58 GC ¶ 224.

[70]Exec. Order No. 11246 (Sept. 24, 1965), 30 Fed. Reg. 12,319 (Sept. 28, 1965), as amended by Exec. Order No. 13672 (July 21, 2014), 79 Fed. Reg. 42,971 (July 23, 2014).

[71]42 U.S.C.A. § 2000e et seq.

[72]81 Fed. Reg. 39,108 n.1 (June 15, 2016); see 41 C.F.R. § 60-1.5 (exemptions).

[73]41 C.F.R. § 60-20.2(a) ("It is unlawful for a contractor to discriminate against any employee or applicant because of sex.").

[74]41 C.F.R. § 60-20.2(a).

[75]41 C.F.R. § 60-20.2(b)(13).

[76]81 Fed. Reg. 39,108, 39,136 (June 15, 2016). The OFCCP has issued guidance about gender identity and transgender status, including definitions and applications to federal contractors. See OFCCP, Dir. 2014-02 (Aug. 19, 2014), https://www.dol.gov/ofccp/regs/compliance/directives/Directive_2014-02.pdf; OFCCP, Frequently Asked Questions: EO 13672 Final Rule, https://www.dol.gov/ofccp/LGBT/LGBT_FAQs.html.

[77]41 C.F.R. § 60-20.5(a).

[78]41 C.F.R. § 60-20.5(a)(2).

[79]41 C.F.R. § 60-20.5(c).

[80]See 81 Fed. Reg. 39,108, 39,129–35 (June 15, 2016) (discussing 41 C.F.R. § 60-20.5).

[81]41 C.F.R. § 60-20.7.

[82]41 C.F.R. § 60-20.7(d)(1).

[83]41 C.F.R. § 60-20.7(a)(1), (2).

[84]41 C.F.R. §§ 60-20.4, 60-20.6.

[85]41 C.F.R. § 60-20.4.

[86]41 C.F.R. § 60-20.4(b), (c).

[87]41 C.F.R. § 60-20.6(b).

[88]41 C.F.R. § 60-20.6(c).

[89]41 C.F.R. § 60-20.1

[90]81 Fed. Reg. 39,108, 39,122 (June 15, 2016).

[91]41 C.F.R. pt. 60-20 app. ("Best Practices").

[92]41 C.F.R. pt. 60-20 app.

[93] 80 Fed. Reg. 54,934 (Sept. 11, 2015) (amending 41 CFR pt. 60-1).

[94]Exec. Order No. 13665 (Apr. 8, 2014), 79 Fed. Reg. 20,749 (Apr. 11, 2014).

[95]80 Fed. Reg. 54,934 (Sept. 11, 2015) (amending 41 CFR pt. 60-1).

[96]41 C.F.R. § 60-1.3.

[97]80 Fed. Reg. 54,934, 54,939 (Sept. 11, 2015); 41 C.F.R. §§ 60-1.4, 60-1.35(c). The DOL's website has a "Pay Transparency" notice poster available at https://www.dol.gov/ofccp/pdf/PayTransparencyNotice_JRFQA508c.pdf.

[98]41 C.F.R. § 60-2.17(b)(3), (c); see 80 Fed. Reg. 54,934, 54,944 (Sept. 11, 2015).

[99]Exec. Order No. 13706 (Sept. 7, 2015), 80 Fed. Reg. 54,697 (Sept. 10, 2015).

[100]81 Fed. Reg. 9592 (Feb. 25, 2016).

[101]81 Fed. Reg. 9592 (Feb. 25, 2016).

[102]81 Fed. Reg. 9592 (Feb. 25, 2016).

[103]81 Fed. Reg. 9592 (Feb. 25, 2016).

[104]81 Fed. Reg. 9592 (Feb. 25, 2016).

[105]DOL, Dir. 2013-02, "Complying With Nondiscrimination Provisions: Criminal Record Restrictions and Discrimination Based on Race and National Origin" (Jan. 29, 2013), available at https://www.dol.gov/ofccp/regs/compliance/directives/dirindex.htm.

[106]DOL, Dir. 2013-02, "Complying With Nondiscrimination Provisions: Criminal Record Restrictions and Discrimination Based on Race and National Origin" 2 (Jan. 29, 2013), available at https://www.dol.gov/ofccp/regs/compliance/directives/dirindex.htm.

[107]DOL, Dir. 2013-02, "Complying With Nondiscrimination Provisions: Criminal Record Restrictions and Discrimination Based on Race and National Origin" 4–5 (Jan. 29, 2013), available at https://www.dol.gov/ofccp/regs/compliance/directives/dirindex.htm.

[108]DOL, Dir. 2013-02, "Complying With Nondiscrimination Provisions: Criminal Record Restrictions and Discrimination Based on Race and National Origin" 5–6 (Jan. 29, 2013), available at https://www.dol.gov/ofccp/regs/compliance/directives/dirindex.htm.

[109]DOL, Dir. 2013-02, "Complying With Nondiscrimination Provisions: Criminal Record Restrictions and Dis-

crimination Based on Race and National Origin" 5 n.3, 8 (Jan. 29, 2013), available at https://www.dol.gov/ofccp/regs/compliance/directives/dirindex.htm.

[110]Exec. Order No. 13673 (July 31, 2014), 79 Fed. Reg. 45309 (Aug. 5, 2014); see 80 Fed. Reg. 30,548 (May 28, 2015) (proposed FAR rule); 80 Fed. Reg. 30,574 (May 28, 2015) (proposed DOL guidance).

[111]81 Fed. Reg. 58,562 (Aug. 25, 2016).

[112]81 Fed. Reg. 58,654 (Aug. 25, 2016).

[113]81 Fed. Reg. 58,652 (Aug. 25, 2016).

[114]81 Fed. Reg. 58,562, 58,640 (Aug. 25, 2016). The rule requires that a contractor disclose whether it has received any labor law decisions, meaning any "administrative merits determination," "arbitral award or decision," or "civil judgments" (as defined in the accompanying guidance) ''rendered against'' it in the three years preceding the date of the offer. 81 Fed. Reg. 58,562, 58,640 (Aug. 25, 2016). The term "administrative merits determination" means certain notices or findings—whether final or subject to appeal or further review—issued by an enforcement agency following an investigation indicating a violation of a labor law. 81 Fed. Reg. 58,562, 58,639 (Aug. 25, 2016). Examples of "administrative merits determinations" include Wage and Hour "Summary of Unpaid Wages" form, Occupational Safety and Health Administration citation, show-cause notice from the OFCCP, complaint issued by a Regional Director at the National Labor Relations Board, and a letter of determination based on reasonable cause from the EEOC. 81 Fed. Reg. 58,654, 58,720–21 (Aug. 25, 2016).

[115]29 U.S.C.A. § 201 et seq.

[116]29 U.S.C.A. § 651 et seq.

[117]29 U.S.C.A. §§ 1801–1872.

[118]29 U.S.C.A. § 151 et seq.

[119]40 U.S.C.A. §§ 3141–3148.

[120]41 U.S.C.A. §§ 6701–6707. See generally Donohue & Goddard, "Complying With the Service Contract Act," Briefing Papers No. 01-9 (Aug. 2001).

[121]Exec. Order No. 11246 (Sept. 24, 1965), 30 Fed. Reg. 12,319 (Sept. 28, 1965).

[122]Exec. Order No. 13658 (Feb. 12, 2014), 79 Fed. Reg. 9851 (Feb. 20, 2014).

[123]29 U.S.C.A. § 793.

[124]38 U.S.C. A. § 4212.

[125]29 U.S.C.A. § 2601 et seq.

[126]42 U.S.C.A. § 2000e et seq.

[127]42 U.S.C.A. § 12101 et seq.

[128]29 U.S.C.A. §§ 621–634.

[129]81 Fed. Reg. 58,654, 58,714, 58,720 (Aug. 25, 2016).

[130]81 Fed. Reg. 58,654, 58,719–20 (Aug 25, 2016).

[131]81 Fed. Reg. 58,562, 58,640 (Aug. 25, 2016).

[132]81 Fed. Reg. 58,562, 58,642–43 (Aug. 25, 2016).

[133]81 Fed. Reg. 58,562, 58,569 (Aug. 25, 2016); 81 Fed. Reg. 58,654, 58,662 (Aug. 25, 2016).

[134]81 Fed. Reg. 58,562, 58,640, 58,643 (Aug. 25, 2016); see 81 Fed. Reg. 58,654, 58,733–34, 58,766–68 (Aug. 25, 2016).

[135]81 Fed. Reg. 58,562 (Aug. 25, 2016); 81 Fed. Reg. 58,654 (Aug. 25, 2016). In addition to these developments, the EEOC also has proposed requiring that contractors collect and report data on pay ranges and hours worked by contractor employees. The EEOC has delayed implementation of this requirement until March 31, 2018. 81 Fed. Reg. 45,479 (July 14, 2016).

[136]81 Fed. Reg. 58,562, 58,588, 58,641 (Aug. 25, 2016); 81 Fed. Reg. 58,654, 58,734 (Aug. 25, 2016).

[137]81 Fed. Reg. 58,562, 58,641–43 (Aug. 25, 2016).

[138]81 Fed. Reg. 58,562, 58,643 (Aug. 25, 2016).

[139]81 Fed. Reg. 58,562, 58,621 (Aug. 25, 2016); 81 Fed. Reg. 58,654, 58,739 (Aug. 25, 2016); Department of Labor, Preassessment (Sept. 6, 2016), https://www.dol.gov/asp/fairpayandsafeworkplaces/PreAssessment.htm.

[140]81 Fed. Reg. 58,562, 58,650–51 (Aug. 25, 2016).

[141]81 Fed. Reg. 58,562, 58,650–51 (Aug. 25, 2016).

[142]81 Fed. Reg. 58,562, 58,651 (Aug. 25, 2016).

[143]PwC, Press Release, "2015 a Record Year for Aerospace & Defense M&A, According to PwC US" (Feb. 9, 2016), available at http://www.pwc.com/us/en/press-releases/2016/pwc-q4-aerospace-defense-ma-press-release.html.

[144]See generally Dover, Horan & Overman, "Mergers & Acquisitions—Special Considerations When Purchasing Government Contractor Entities/Edition II," Briefing Papers No. 09-7 (June 2009).

[145]FAR 42.1204(b).

[146]Universal Protection Serv., LP v. United States, 126 Fed. Cl. 173 (2016).

[147]FCi Fed., Inc., Comp. Gen. Dec. B-408558.7 et al., 2015 CPD ¶ 245, 57 GC ¶ 298.

[148]Wyle Labs., Inc., Comp. Gen. Dec. B-408112.2, 2014 CPD ¶ 16, 56 GC ¶ 39.

[149]Nat'l Aeronautics & Space Admin.—Recons., Comp. Gen. Dec. B- 408112.3, 2014 CPD ¶ 155.

[150]IBM U.S. Fed., Div. of IBM Corp., Comp. Gen. Dec. B-409806 et al., 2014 CPD ¶ 241.

[151]VSE Corp.—Costs, Comp. Gen. Dec. B-407164.11 et al., 2014 CPD ¶ 202.

[152]IBM U.S. Fed., Div. of IBM Corp., Comp. Gen. Dec. B-409806 et al., 2014 CPD ¶ 241.

[153]Dell Servs. Fed. Gov't, Inc., Comp. Gen. Dec. B-412340 et al., 2016 CPD ¶ 43.

[154]See Dell Servs. Fed. Gov't, Inc., Comp. Gen. Dec. B-412340 et al., 2016 CPD ¶ 43, at *6 n.7. ("Moreover, to the extent the awardee would rely on any resources of a corporate parent, the protester has made no showing that the relevant corporate resources would be spun off to the printer

and personal devices company, rather than to the Hewlett Packard Enterprise Company, which will focus on the types of enterprise solutions offered by the awardee, and which will be the new corporate parent of the awardee.").

[155]Veterans Evaluation Servs., Inc., Comp. Gen. Dec. B-412940 et al., 2016 CPD ¶ 185.

[156]Veterans Evaluation Servs., Inc., Comp. Gen. Dec. B-412940 et al., 2016 CPD ¶ 185, at *10 ("Simply stated, there is no basis to object to the agency's evaluation of the QTC proposal for failing to take into consideration a transaction that has not occurred, and that may not have any effect on QTC's ability to perform.").

