VENABLE® LLP

Government Contracts Symposium

April 10, 2014

8:00 a.m. – 4:00 p.m.

Venable LLP
575 7th Street, NW
Washington, DC 20004



VENABLE LLP WELCOMES YOU TO OUR SECOND ANNUAL

Government Contracts Symposium

8:00 a.m. - 8:30 a.m.	Networking and Continental Breakfast
8:30 a.m. - 8:40 a.m.	Welcome and Opening Remarks

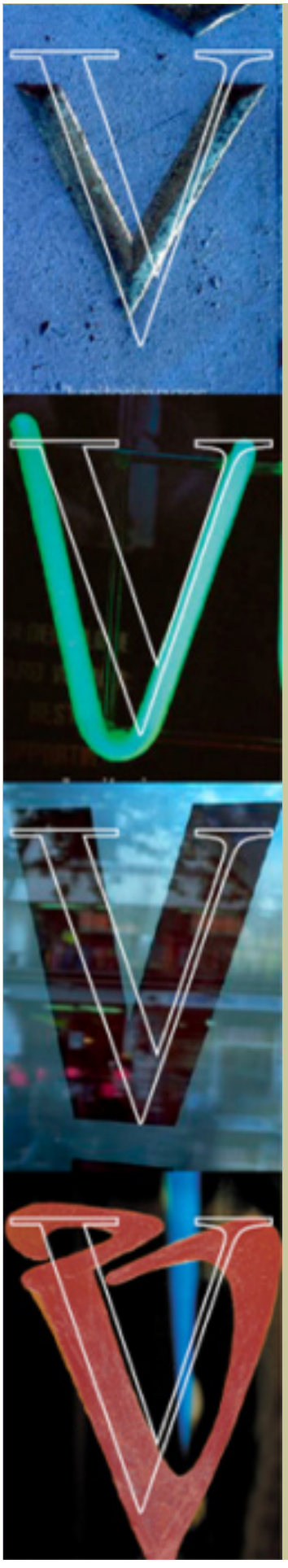
Morning Session

8:40 a.m. - 9:40 a.m.	Changes to the Small Business Rules
9:50 a.m. - 10:50 a.m.	Protecting Against the Government's Administrative Remedies
11:00 a.m. - 12:00 p.m.	Strategies for Managing and Mitigating Risk in Government Contracts
12:00 p.m. - 12:20 p.m.	Lunch
12:20 p.m. - 12:50 p.m.	Keynote Address: Sharon L. Larkin, "Surviving (and Perhaps Thriving) in the Federal Procurement Law Headwinds"

Afternoon Session

1:00 p.m. - 2:00 p.m.	Ethics and Compliance in a Heightened Enforcement Environment
2:10 p.m. - 3:00 p.m.	Cyber Pros and Cons for Government Contractors
3:10 p.m. - 4:00 p.m.	Hot Topics in Government Contracts
4:00 p.m.	Closing Remarks and Reception

VENABLE® LLP



Changes to the Small Business Rules

8:40 a.m. – 9:40 a.m.

Lars E. Anderson, Venable LLP

Keir X. Bancroft, Venable LLP

Kimberly deCastro, Wildflower

Kenneth Dodds, Small Business Administration

Melanie Jones Totman, Venable LLP

VENABLE® LLP

VENABLE® LLP

Changes to the Small Business Rules

APRIL 10, 2014

VENABLE® LLP

Agenda

- New SBA subcontracting requirements
  - Small Business Contracting, 78 Fed. Reg. 42391, July 16, 2013
  - Amending 13 C.F.R. Parts 121, 125
- Small business fraud
  - Size and Status Integrity, 78 Fed. Reg. 38811, June 28, 2013
  - Amending 13 C.F.R. Parts 121, 124, 125, 127
- Practical implications and suggested guidance

VENABLE LLP

Melanie Jones Totman – Moderator

Melanie Jones Totman is an associate with Venable's Government Contracts team, where she provides clients with legal advice related to both federal and state procurement law, including complex compliance matters under the Federal Acquisition Regulation, the Office of Management and Budget Circulars and various state procurement laws and regulations. She generally advises clients on small business, False Claims Act, and mandatory disclosure issues. She represents clients in a variety of bid protests before the United States Government Accountability Office and the United States Court of Federal Claims.

Ms. Totman has broad experience in the defense of audits by various Offices of Inspector General and the Defense Contract Audit Agency. Some of Ms. Totman's work includes:

- Successfully appealing a small business size determination before the United States Small Business Administration, Office of Hearings & Appeals. *Size Appeal of GPA Technologies, Inc.*, SBA No. SIZ-5307 (2011).
- Successfully defending a small business size determination before the United States Small Business Administration, Office of Hearings & Appeals. *Size Appeals of BA Urban Solutions et al.*, SBA No. SIZ-5521 (2013).
- Defending large contractors, nonprofit organizations, and state agencies awarded federal grant funds in audits by the Department of Homeland Security, Office of Inspector General; the Department of Transportation, Office of Inspector General; and the Department of Defense Inspector General.

VENABLE LLP

Kimberly deCastro – Panelist

Kimberly deCastro is Wildflower's President and CEO. Since founding Wildflower in 1991, she has delivered world-class products and services to the U.S. government and its prime contractors, with a philosophy of constant improvement for the company, its business partners, and the community. Her policy of "yes we can" informs Wildflower's organizational approach to its customers and their satisfaction. Kimberly has nearly 30 years of experience working with the public sector. A working CEO, Kimberly has personally managed several large programs since founding the company. Prior to 1991, Kimberly was the National Sales Director at Mechanics Choice, an industrial division of Avnet. From 1985 until 1991, she directed a sales force of 400 employees across the U.S. Kimberly attended the United States International University in San Diego, CA and the University of Hawaii. She is cleared (current, active) to Top Secret.

VENABLE LLP

Kenneth Dodds – Panelist

Kenneth Dodds is the Director of Procurement Policy and Liaison at the Small Business Administration (SBA). His office is responsible for implementing legislation and drafting regulations pertaining to small business Federal government contracting programs and size standards. Previously he served as the Director, Office of Government Contracting and as a senior attorney in SBA's Office of General Counsel. He is a graduate of James Madison University and received his law degree from the College of William & Mary.

VENABLE LLP

Lars E. Anderson – Panelist

In 43 years in the field, including 15 years as a Navy procurement attorney, Lars Anderson has handled virtually every issue that arises in contracting and doing business with the federal government. Clients rely on him for:

- assistance during the competitive bid process
- defense or prosecution of bid protests
- help in complying with regulations and laws during contract performance
- resolution of disputes and claims during contract performance
- resolution of claims as a result of contract termination

His experience includes resolving disagreements over highly technical specifications – including changed conditions, delays or disruption in construction, manufacture or maintenance of weapons systems and equipment, and allegations regarding violations of procurement integrity laws.

His experience encompasses, among other areas:

- Aerospace – maritime
- Electronics – OMB A-76 competitions
- Travel – Information technology
- All aspects of small business programs

He also assists contractors in performing risk analysis and developing proposals.

Keir X. Bancroft – Panelist

Keir Bancroft provides a range of services to government contractors. Mr. Bancroft represents clients in litigation, including bid protests, size and status protests, and contract-related disputes before tribunals including the GAO, the SBA, boards of contract appeal and the United States Court of Federal Claims.

Mr. Bancroft also drafts and negotiates subcontracts, nondisclosure agreements, joint ventures, mentor-protégé agreements, and licensing agreements on behalf of clients.

Within the broad rubric of cybersecurity, Mr. Bancroft specializes in information security and privacy compliance. He helps clients comply with standards under the Federal Information Security Act (FISMA), the Department of Defense Information Assurance guidelines, the Privacy Act, and similar requirements. Mr. Bancroft also focuses on national security and industrial security issues arising under the National Industrial Security Program Operating Manual (NISPOM).

Before joining private practice, Mr. Bancroft served as an attorney advisor and the Privacy Officer in the United States Department of the Treasury, Bureau of Engraving and Printing. There, he counseled and represented the Bureau in all facets of federal procurement and was responsible for ensuring Bureau systems complied with privacy and information security requirements.

.

Subcontracting

- 78 Fed. Reg. 42391 (July 16, 2013)
- Prime must notify CO when it fails to pay sub within 90 days, where sub has completed performance and prime has been paid.
- Prime must notify CO when prime used sub to prepare offer, but not in performance.
- CO may consider as part of past performance.
- Firm with history of late payment may be reported in FAPIIS.

Subcontracting

- Subcontracting in Source Selection
- CO may include evaluation factor that considers and compares:
  - Prime's proposed approach to subcontracting
  - The extent to which Prime met subcontracting goals under prior contracts
  - The extent to which Prime timely paid subcontractors under prior contracts
  - Prime's commitment to pay subcontractors within a specified number of days

New Subcontracting Requirements

- "Maximum Practicable Opportunity"
  - Prime must undertake market research to identify small business subcontractors and suppliers through "all reasonable means."
  - Under large awards, Primes must give pre-award written notice to unsuccessful SB subcontractors.
  - No prohibition on subcontractors discussing *material matters* of prime utilization with CO.

New Subcontracting Requirements – Practical Implications

- Carefully negotiate teaming agreements.
  - Know your teaming partners.
  - Clearly define expectations for your relationship.
- Past Performance ratings could suffer for failure to meet stated subcontracting plans.

New Subcontracting Requirements – Protecting a Subcontractor Position

- Clearly document expectations with your Prime contractor on the percentage, nature, and scope of work.
- Know the CO for each contract.
- Define bright-line expectations for mechanics of payment.

New Subcontracting Requirements – Protecting a Subcontractor Position

- Establish a protocol for contesting a delay or reduction in payment:
  - Immediately communicate concerns with delayed payments in writing in order to start the 90-day clock.
  - Maintain open communications with the Prime on the potential for immediate partial payment for undisputed amounts.
  - Educate personnel on when to contact counsel.
  - Determine when to approach CO on "material matters" pertaining to payment or utilization.

New Subcontracting Requirements – Protecting a Prime Contractor Position

- Document any and all efforts to follow the proposal.
- Establish a clear audit trail for deviations from the subcontracting plan or proposal, explaining the specific reasons for deviations and how the deviation is advantageous to the government and/or other SBs.
- Promptly notify the CO of such reasons in writing and document the CO's response.

New Subcontracting Requirements – Protecting a Prime Contractor Position

- Develop a plan for how to deal with a discrepancy in payment owed to a subcontractor:
  - Who will communicate with the subcontractor?
  - Who will communicate with the CO?
  - At what point should your personnel call counsel?
  - Develop a template plan to present to the CO for resolving differences.
  - Include an agreed-to resolution plan in teaming agreements and subcontracts.

Size Standards

- SBA Establishes size standards for North American Industry Classification System (NAICS) codes
- Small Business = not dominant in its field of operation
- Services/Construction - average annual revenue over three previously completed fiscal years
  - Range is $7 million to $35.5 million
- Manufacturers or Non-manufacturers – average number of employees over three previously completed calendar months
  - Range is 500 to 1,500 employees
- SBA must review all size standards every 5 years

Size Standards

- Solicitation should have single NAICS code and size standard (13 CFR 121.402)
  - Unless multiple award, CLINs
- Size Standard change before offers are due, CO must amend Solicitation (13 CFR 121.402)
- Interested parties may protest NAICS code/size standard designations to SBA's Office of Hearings and Appeals
  - 13 CFR 121.1101-1103, 134.301-318

Size Determination

- SBA determines the size status of a concern, including its affiliates, as of the date the concern submits a written self-certification that it is small to the procuring agency as part of its initial offer (or other formal response to a solicitation), which includes prices. 13 CFR 121.404(a)
- In determining the concern's size, SBA counts the receipts, employees, or other measure of size of the concern whose size is at issue, and all of its domestic and foreign affiliates, regardless of whether the affiliates are organized for profit. 13 CFR 121.103(a)(6)

Affiliation – 13 CFR 121.103

- Concerns and entities are affiliates of each other when one controls or has the power to control the other, or a third party (or parties) controls or has the power to control both. It does not matter whether control is exercised, as long as the power to control exists.

Affiliation

- SBA considers factors such as ownership, management, previous relationships with or ties to another concern, and contractual relationships, in determining whether affiliation exists.
- Control may be affirmative or negative.
- A firm will not be treated as a separate business concern if a substantial portion of its assets and/or liabilities are the same as those of a predecessor entity. In such a case, the annual receipts and employees of the predecessor will be taken into account in determining size. 13 CFR 121.105(c)

VENABLE LLP

Annual Representations and Certifications

(d) The offeror has completed the annual representations and certifications electronically via the SAM website accessed through https://www.acquisition.gov. After reviewing the SAM database information, the offeror verifies by submission of the offer that the representations and certifications currently posted electronically that apply to this solicitation as indicated in paragraph (c) of this provision have been entered or updated within the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard applicable to the NAICS code referenced for this solicitation), as of the date of this offer and are incorporated in this offer by reference (see FAR 4.1201); except for the changes identified below [*offeror to insert changes, identifying change by clause number, title, date*]. These amended representation(s) and/or certification(s) are also incorporated in this offer and are current, accurate, and complete as of the date of this offer.

- FAR 52.204-8

VENABLE LLP

Presumption of Loss

In every contract, subcontract, cooperative agreement, cooperative research and development agreement, or grant which is set aside, reserved, or otherwise classified as intended for award to small business concerns, there shall be a presumption of loss to the United States based on the total amount expended on the contract, subcontract, cooperative agreement, cooperative research and development agreement, or grant whenever it is established that a business concern other than a small business concern willfully sought and received the award by misrepresentation.

- 15 USC 632(w)

Deemed Certifications

The following actions shall be deemed affirmative, willful, and intentional certifications of small business size and status:

- (A) Submission of a bid or proposal for a Federal grant, contract, subcontract, cooperative agreement, or cooperative research and development agreement reserved, set aside, or otherwise classified as intended for award to small business concerns.
- (B) Submission of a bid or proposal for a Federal grant, contract, subcontract, cooperative agreement, or cooperative research and development agreement which in any way encourages a Federal agency to classify the bid or proposal, if awarded, as an award to a small business concern.
- (C) Registration on any Federal electronic database for the purpose of being considered for award of a Federal grant, contract, subcontract, cooperative agreement, or cooperative research agreement, as a small business concern.

– 15 USC 632(w)(2)

Limitation of Liability – Safe Harbors

- Error or misrepresentation
- Unintentional errors
- Technical malfunctions
- "Other similar situations" demonstrating misrepresentation was not affirmative, intentional, or actionable under False Claims Act

Limitation of Liability – Safe Harbors

Paragraphs (a) through (c) of this section may be determined not to apply in the case of unintentional errors, technical malfunctions, and other similar situations that demonstrate that a misrepresentation of size was not affirmative, intentional, willful or actionable under the False Claims Act, 31 U.S.C. § § 3729, et seq.

- 13 CFR 121.108(d)

Limitation of Liability – Safe Harbors

A prime contractor acting in good faith should not be held liable for misrepresentations made by its subcontractors regarding the subcontractors' size.

- 13 CFR 121.108(d)

Limitation of Liability – Safe Harbors

Relevant factors to consider in making this determination may include the firm's internal management procedures governing size representation or certification, the clarity or ambiguity of the representation or certification requirement, and the efforts made to correct an incorrect or invalid representation or certification in a timely manner.

– 13 CFR 121.108(d)

Limitation of Liability – Safe Harbors

An individual or firm may not be held liable where government personnel have erroneously identified a concern as small without any representation or certification having been made by the concern and where such identification is made without the knowledge of the individual or firm.

– 13 CFR 121.108(d)

Suspension and Debarment

The SBA suspension and debarment official or the agency suspension and debarment official may suspend or debar a person or concern for misrepresenting a firm's size status pursuant to the procedures set forth in 48 CFR subpart 9.4.

– 13 CFR 121.108(e)(1)

Civil Penalties

Persons or concerns are subject to severe penalties under the False Claims Act, 31 U.S.C. 3729-3733, and under the Program Fraud Civil Remedies Act, 331 U.S.C. 3801-3812, and any other applicable laws.

– 13 CFR 121.108(e)(2)

Criminal Penalties

Persons or concerns are subject to severe criminal penalties for knowingly misrepresenting the small business size status of a concern in connection with procurement programs pursuant to section 16(d) of the Small Business Act, 15 U.S.C. 645(d), as amended, 18 U.S.C. 1001, 18 U.S.C. 287, and any other applicable laws. Persons or concerns are subject to criminal penalties for knowingly making false statements or misrepresentations to SBA for the purpose of influencing any actions of SBA pursuant to section 16(a) of the Small Business Act, 15 U.S.C. 645(a), as amended, including failure to correct "continuing representations" that are no longer true.

– 13 CFR 121.108(e)(3)

Criminal Penalties

- Also applies to HUBZone, 8(a), SDB, WOSB, SDVO
- Fine of not more than $500,000 and imprisonment for not more than 10 years, or both
- Sections 8(m)(5)(C), 16(d) and 36(d) of the Small Business Act, 15 USC 637(m)(5)(C), 645(d), and 657f(d)
- Final Rule 78 Fed. Reg. 38811 (June 28, 2013)

Size and Status Integrity – Exposing Fraud

- Size Protest at the Small Business Administration (SBA)
- Notify appropriate contracting officer of current procurement
- Notify procuring agency and SBA Inspector General

Size and Status Integrity – Suggested Guidance

- Designate a compliance officer to sign each representation who understands how to calculate size and status under the rules.
- Document rationale for determining size as it relates to the rules. Include that rationale in your certification. Do not rely on SAM.
- When in doubt, call outside counsel!

VENABLE LLP

Contact Information

Lars E. Anderson
leanderson@Venable.com
t 703.760.1605
f 703.821.8949

Keir X. Bancroft
kxbancroft@Venable.com
t 202.344.4826
f 202.344.8300

Melanie Jones Totman
mjtotman@Venable.com
t 202.344.4465
f 202.344.8300

Kenneth Dodds
Director, Policy, Planning & Liaison
Small Business Administration
kenneth.dodds@sba.gov
t 202.619.1766

www.Venable.com

Additional Information

Exhibit 1:

Small Business Contracting, 78 Fed. Reg. 42391, July 16, 2013

Product class	Energy efficiency ratio, effective from Oct. 1, 2000 to May 31, 2014	Combined energy efficiency ratio, effective as of June 1, 2014
11. With reverse cycle, with louvered sides, and less than 20,000 Btu/h	9.0	9.8
12. With reverse cycle, without louvered sides, and less than 14,000 Btu/h	8.5	9.3
13. With reverse cycle, with louvered sides, and 20,000 Btu/h or more	8.5	9.3
14. With reverse cycle, without louvered sides, and 14,000 Btu/h or more	8.0	8.7
15. Casement-Only	8.7	9.5
16. Casement-Slider	9.5	10.4

* * * * *

[FR Doc. 2013–17005 Filed 7–15–13; 8:45 am]
BILLING CODE 6450–01–P

SMALL BUSINESS ADMINISTRATION

13 CFR Parts 121 and 125

RIN 3245–AG22

Small Business Subcontracting

AGENCY: U.S. Small Business Administration.

ACTION: Final rule.

SUMMARY: The U.S. Small Business Administration (SBA or Agency) is amending its regulations governing small business subcontracting to implement provisions of the Small Business Jobs Act of 2010. In particular, this rule adds a provision providing that for a "covered contract" (a contract for which a small business subcontracting plan is required), a prime contractor must notify the contracting officer in writing whenever the prime contractor does not utilize a small business subcontractor used in preparing its bid or proposal during contract performance. This rule also adds a provision requiring a prime contractor to notify a contracting officer in writing whenever the prime contractor reduces payments to a small business subcontractor or when payments to a small business subcontractor are 90 days or more past due. In addition, this rule clarifies that the contracting officer is responsible for monitoring and evaluating small business subcontracting plan performance. The rule also clarifies which subcontracts must be included in subcontracting data reporting, which subcontracts should be excluded, and the way subcontracting data is reported. The rule also makes changes to update its subcontracting regulations, including changing subcontracting plan thresholds and referencing the electronic subcontracting reporting system (eSRS). Further, the rule adds a provision to the regulations which addresses subcontracting plan requirements and credit towards subcontracting goals in connection with multiple award multi-agency, Federal Supply Schedule, Multiple Award Schedule and government-wide acquisition indefinite delivery, indefinite quantity contracts.

DATES: *Effective Date:* This rule will be effective August 15, 2013.

FOR FURTHER INFORMATION CONTACT: Dean Koppel, U.S. Small Business Administration, Office of Government Contracting, 409 Third Street SW., 8th Floor, Washington, DC 20416, (202) 205–7322, *dean.koppel@sba.gov*.

SUPPLEMENTARY INFORMATION: On October 5, 2011, SBA published in the **Federal Register** a proposed rule to implement provisions of the Jobs Act which pertain to small business subcontracting. 76 FR 61626. Section 1321 of the Jobs Act requires the SBA Administrator, in consultation with the Administrator of the Office of Federal Procurement Policy, to publish regulations establishing policies for subcontracting compliance, including assignment of compliance responsibilities between contracting offices, small business offices, and program offices.

The proposed rule called for a 60-day comment period, with comments to be received by SBA by December 5, 2011. SBA published a notice in the **Federal Register** on December 1, 2011, reopening the comment period for an additional 30 days, until to January 6, 2012. 76 FR 74749.

The proposed rule contained changes to SBA's size regulations (Part 121) and the regulations governing SBA's government contracting programs (Part 125). SBA received 105 written comments during the comment period. Many of these comments were lengthy and discussed numerous proposed amendments. SBA has made changes in this final rule in response to comments received to its notice of proposed rulemaking. With the exception of comments which are beyond the scope of this rule, or which did not set forth any rationale or make suggestions, SBA discusses and responds fully to all of the comments below.

Summary of Comments and SBA's Responses

Part 121

SBA received one comment on proposed § 121.404(g)(3)(ii), which added a provision permitting a contracting officer to require a subcontracting plan if a prime contractor's size status changes from small to other than small as a result of a size recertification. The commenter recommended adding that size status at time of contract award controls subcontracting plan requirements or clarifying how a subcontracting plan must change if a former small business subcontractor reclassifies. Section 121.404(g)(3)(ii) provides that recertification does not change the terms and conditions of a contract, including the requirement for a subcontracting plan, and otherwise size is determined at time of offer and will not change during performance. However, under the final rule a contracting officer has the discretion to require a subcontracting plan if size status changes as a result of recertification.

Part 125

The proposed rule revised § 125.3(a) to update the subcontracting plan thresholds, which were increased pursuant to the government-wide procurement program inflationary adjustments required by Section 807 of the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005, Public Law 108–375; *see also* 75 FR 53129 (Aug. 30, 2010). One commenter recommended removing the reference to "a public facility" in § 125.3(a) because the term is not defined in the Code of Federal Regulations. SBA does not adopt this comment. It is up to the contracting officer to determine whether the term applies to a particular acquisition. Further, this term comes from Section 8(d) of the Small Business Act, so removing it would require legislative action.

The proposed rule added § 125.3(a)(1) to define subcontract in order to clarify which subcontracts must be included when reporting on small business subcontracting performance. SBA

received a number of comments on proposed § 125.3(a)(1). Many commenters supported SBA's definition of a subcontract.

One commenter requested confirmation that the new definition of subcontract will be coordinated with existing definitions at Federal Acquisition Regulation (FAR) 19.701 and FAR 52.219–9. SBA agrees that it is important for SBA's rules and the FAR to be consistent and notes that its rules will also be incorporated in the FAR after SBA's regulations are finalized.

One commenter requested that SBA clarify how subcontracts to and by affiliates will be treated. SBA's long-standing policy has been to count subcontracts by first-tier affiliates as subcontracts of the prime contractor. SBA has amended § 125.3(a)(1) to make this clear. SBA notes that the Subcontracting Report for Individual Contracts (ISR) (SF–294) and the Summary Subcontract Report (formerly the SF–295, now discontinued) and their electronic equivalents in eSRS specifically state that subcontracts to affiliates are not included in the individual and summary reports.

One commenter recommended excluding bonds and all insurance from the definition of subcontract. The commenter noted that in the construction industry, prime contractors generally have established and ongoing relationships with sureties and insurance providers, and bond and insurance requirements are generally met through these relationships, so no real opportunity for small business exists in those areas. The commenter also noted that the government's requirements for bonds and insurance—specifically for construction contracts—normally preclude the use of small business concerns. Although SBA is sympathetic to this comment, SBA would need more information on the participation of small business concerns in these industries before excluding bonds and all insurance from the subcontracting base government-wide.

One commenter opposed excluding philanthropic contributions from the definition of subcontract. The commenter noted that on Department of Defense contracts, services provided to the prime contractor by Historically Black Colleges and Universities (HBCUs) are generally funded by a donation or grant rather than charged, and excluding such donations/grants undermines a prime contractor's ability to support such HBCUs. SBA disagrees. It is unclear how a philanthropic contribution could be counted as a subcontract and charged to the government.

One commenter recommended requiring transparency in calculating the subcontracting base, arguing that the prime contractor has too much discretion and there are no checks in place. SBA does not concur. By statute, the contracting officer is responsible for negotiating a subcontracting plan that maximizes small business participation and for monitoring performance. SBA and contracting agencies also monitor subcontracting plan compliance through compliance reviews.

One commenter recommended requiring discrete subcontracting reports, rather than comprehensive reports, for all prime contracts of $1 million or more. SBA notes that comprehensive plans are authorized by statute and that commercial plans are authorized by the FAR. In addition, the thresholds for subcontracting plan reports are set by statute.

Several commenters opposed the exclusion of utilities from the subcontracting base. One commenter argued that electricity and other utilities should be included in the subcontracting base because small business concerns may be licensed or otherwise equipped to provide these services. Another commenter suggested that the exclusion should be more specifically defined to exclude services that are not required municipal services such as those required under local franchise agreements. SBA has amended the rule to exclude utilities where no competition exists and thus no small business concern could have an opportunity to receive a subcontract. Specifically, SBA has amended the definition to exclude "utilities such as electricity, water, sewer and other services purchased from a municipality or solely authorized by the municipality to provide those services in a particular geographical region." Another commenter argued that not including utilities in the subcontracting base causes an overstatement of the percentage of contracts given to small business. Subcontracting plans are required to the extent subcontracting possibilities exist. As stated above, SBA has amended the rule to clarify that utilities are only excluded to the extent there is no choice of provider.

One commenter recommended clarifying that the supplies or services provided under the agreement must be specific to the particular prime contract requirements in order for the agreement to be considered a subcontract. Specifically, the commenter believed it would be useful to clarify that an agreement to obtain supplies or services that are in the nature of commercial items and are used to support both commercial and government contracts would not be considered a "subcontract." The commenter is further requesting clarification concerning whether subcontracting flowdown requirements apply to certain types of contracts. As the commenter notes, certain vendor agreements must be included in the subcontracting base for commercial plans because those plans are required to consider indirect costs. Further, FAR 52.219–9(j) addresses flowdown requirements in the context of commercial items. Consequently, we have declined to address this matter in the final rule.

One commenter recommended clarifying if the list of exclusions is exhaustive or illustrative. SBA agrees and has amended the rule to state that the list "includes but is not limited to."

One commenter recommended clarifying whether vendors of commercial items are subcontractors for flow-down clauses. SBA has clarified that flow-down clauses apply to commercial item vendors, except when the subcontract is for a commercial item and the prime contract contains FAR clause 52.212–5 or 52.244–6. Under this scenario, the prime contractor is required to flow down FAR clause 52.219–8 but not the clause at 52.219–9; accordingly, no subcontracting plan is required from other than small subcontractors at any tier (*see* Federal Acquisition Streamlining Act of 1994, Pub. L. 103–355, and FAR 52.219–9(j), 52.212–5(e), and 52.244–6(c)).

One commenter requested clarification of whether contracts in connection with foreign military sales are subject to the subcontracting plan requirements of the Small Business Act and the FAR. Based on the proposed definition, which SBA is adopting, contracts in connection with foreign military sales are subject to the subcontracting plan requirements, unless this requirement is waived in accordance with the procuring agency's regulations. Specific questions concerning specific contracts should be directed to the contracting officer.

The proposed rule added § 125.3(a)(2) to explicitly authorize contracting officers to establish additional subcontracting goals in terms of total contract dollars. As explained in the proposed rule, contracting officers are already doing this, and when a prime contractor enters its subcontracting achievements (i.e., dollars) into eSRS, the system automatically calculates the percentage by both methods—that is, as a percentage of total subcontracting and as a percentage of total contract dollars. Thus, the contracting officer has the ability to compare achievements against

the total contract dollars if desired. Several commenters supported SBA's proposal to allow contracting officers to set additional subcontracting goals in terms of total dollars.

One commentor opposed proposed § 125.3(a)(2), arguing that the change would result in the illusion that there are more subcontracting opportunities for small businesses than in fact exist. The commenter argued under some contracts more than 70% of total contract dollars are spent on personnel expenses related to salary and benefits, which are costs for which there are no subcontracting opportunities. However, the commenter noted that the contracting officer has the ability to compare achievements either way (percent of subcontracting dollars or percent of total contract dollars) because eSRS automatically calculates percentage by both methods when prime contractors report achievements in whole dollars. Thus, SBA believes that contracting officers should have the discretion to set goals in terms of total contract dollars. Some contracting officers already set current goals in terms of total contract dollars, and as the commenter notes, the calculation is already available in eSRS. Contracting officers need to set realistic goals, taking into account the opportunity for subcontracting and the percentage of dollar value that accrues to personnel expenses. However, subcontracts for labor are counted towards the total dollar contract value. SBA does not want to limit contracting officer flexibility that benefits small businesses.

One commenter questioned whether under the amended rule, small business goals set in terms of percentage of subcontracting dollars would be evaluated in terms of percentage of total contract dollars. SBA notes that the goals still must be set in terms of percentage of subcontracting dollars, but can be set in terms of total contract dollars as well.

The proposed rule added § 125.3(a)(3) to define a history of unjustified untimely or reduced payments as three incidents within a 12 month period. SBA invited comments on the proposed definition, alternatives with supporting rationales, and/or comments on whether such judgments should be left to the discretion of the contracting officer. SBA received several comments on the proposed definition of a history of unjustified late payment. Some commenters recommended that the definition should look for patterns, as opposed to specific numbers. Others recommended defining it based on percentages, and others recommend establishing a dollar value threshold. Others asked SBA to define when a payment that is late is unjustified. Some commenters argued that it should be left in the discretion of the contracting officer.

SBA has decided to retain the proposed definition of three payments in a twelve month period that are more than 90 days past due, after performance has occurred and the government has paid the prime contractor, where the late payment is unjustified. If a payment is late but it is justified in the opinion of the prime contractor, e.g., unacceptable or incomplete performance, then the late payment would be justified, and there would be no requirement to notify the contracting officer. On the other hand, if satisfactory performance by the subcontractor has occurred, the prime contractor has been paid by the government, and payment to the subcontractor is more than 90 days past due, the prime contractor owes the contracting officer an explanation, regardless of the dollar value of the contract. The statute stipulates that payment to a subcontractor after 90 days is unacceptable unless justified. Further, looking for patterns or percentages would overly complicate a fairly simple principle: if satisfactory performance has occurred and the prime has been paid, subcontractors must be paid within 90 days.

Additional Responsibilities of Large Prime Contractors

The proposed rule amended the introductory text of § 125.3(c)(1) to reflect the updated subcontracting plan thresholds, as discussed above. One commenter opposed changing the thresholds, arguing that the higher the thresholds, the less small business participation will occur because small businesses are not required to submit subcontracting plans. However, the thresholds are set by statute, and subcontracting plans require percentages that are realistic based on subcontracting opportunity.

One commenter recommended amending § 125.3(c)(1)(i) to require prime contractors to give at least 30% of contracts to small business subcontractors. SBA disagrees. Subcontracting plans are established based on small business subcontracting opportunity. It would be inefficient and unfair to establish thresholds that would apply to all contracts government-wide.

SBA proposed to amend § 125.3(c)(1)(iii) to provide that a prime contractor may not prohibit a subcontractor from discussing with the contracting officer any material matter pertaining to payment or utilization. Some commenters argued that the proposed change conflicts with the principle of privity of contract. SBA disagrees. The contracting officer will not take any action with respect to the subcontractor. Rather, the contracting officer can take action with respect to the prime contractor's performance, which is the purpose of the statutory provisions. Other commenters argued that the contracting officer will become the entry point for contract disputes between primes and subcontractors. SBA notes that the contracting officer cannot be a party to disputes between subcontractors and prime contractors but must be involved in evaluating prime contractors' performance.

SBA received several comments on proposed § 125.3(c)(1)(iv), which provided that when preparing its individual subcontracting plan, a prime contractor must decide whether or not to include indirect costs in the subcontracting base, for both goaling and reporting purposes. Some commenters argued that this change would be an administrative burden on contractors and would not further the goals of the program. In proposing this rule, SBA's intent was to memorialize current practice. As explained in the proposed rule, indirect costs must be included in a commercial plan to ensure comparability between goals and achievements because companies with commercial plans file only a summary report, not an individual report. All contractors must include indirect costs in their summary subcontracting reports.

As discussed in the proposed rule, § 125.3(c)(1)(iv) is being amended to reflect current practice.

One commenter recommended providing a specific definition for "indirect cost" as it pertains to small business subcontracting plans and eSRS reporting. The commenter noted that the definition in FAR Part 2 is vague and does not work well in this context. SBA disagrees. For consistency, SBA uses the FAR definition. SBA notes that requests to change the FAR should be directed to the FAR Council.

SBA proposed to add § 125.3(c)(1)(v), providing that large prime contractors are responsible for assigning NAICS codes and corresponding size standards to subcontracts. In response to comments, SBA has amended proposed § 125.3(c)(1)(v) to clarify that in assigning NAICS codes to subcontracts, prime contractors should use the guidance in SBA's regulations governing contracting officers' assignment of NAICS codes to prime contractors, 13 CFR 121.410. In addition, SBA has amended the regulation to clarify that prime contractors may rely on

subcontractors' electronic representations and certifications made in the System for Award Management (SAM) (or any successor system), provided the subcontract contains a clause similar to current FAR clause 52.204–8(d) which clearly provides that the subcontractor is representing its size or socioeconomic at the time of offer for the subcontract. However, SBA notes that SAM was created for firms that want to do business with the government as prime contractors, and some subcontractors may not want to enter data into SAM. As such, SBA has also clarified that a prime contractor (or subcontractor) may not require the use of SAM (or a successor system) for size or socioeconomic representation for subcontracts.

One commenter recommended clarifying whether § 125.3(c)(1)(v) applies to all subcontractors or only to certified small business subcontractors. The commenter also inquired as to whether a list of applicable NAICS codes would be provided at the time of proposal request. The assignment of a NAICS code and size standard is required for subcontracts, since that forms the basis for the prime contractor's claim that it awarded a subcontract to a small business or an other than small business. The prime contractor must assign a NAICS code to the solicitation, so that the subcontractor can make a size or socioeconomic representation in connection with that offer for that subcontract. Size or socioeconomic status is determined as of the date of offer for the subcontract.

The proposed rule amended redesignated § 125.3(c)(1)(vi) (former § 125.3(c)(1)(iii)) to provide that all contractors whose reports are rejected, including those with individual contract plans and commercial plans as defined in FAR 19.701, will be required to make the necessary corrections and resubmit their reports within 30 days of receiving the notice of rejection.

One commenter recommended that the rule refer to eSRS "or the successor system," arguing that eSRS is being replaced by SAM. In response to the comment, SBA has added clarifying language to the regulation.

One commenter recommended allowing 60 days to correct a report. SBA disagrees. Thirty days should be sufficient. One of the reasons for the Jobs Act was the belief that contracting officers and prime contractors are not reporting or reviewing subcontracting accomplishments in a timely manner.

One commenter recommended adding specific consequences for a prime contractor's failure to submit timely or accurate required reports. SBA does not concur. It is difficult to establish concrete, universally applicable consequences for contracting officers and prime contractors. SBA believes that compliance by the contracting officer or prime contractor could be considered as part of the performance evaluation of either party, at the discretion of the evaluator.

One commenter recommended adding a provision addressing the frequency and nature of the subcontracting reports that must be submitted to the contracting officer. SBA notes that these issues are addressed in the FAR.

One commenter recommended fixing data input and error issues in the eSRS system so the necessary data for enforcement can be available. In response to this comment, SBA recommends that contracting agencies include data quality as part of the performance evaluation of employees.

One commenter recommended reviewing eSRS and the Federal Funding Accountability and Transparency Act (FFATA) Subaward Reporting System (FSRS) databases and eliminating duplicate reporting requirements. SBA notes that FSRS is the reporting tool required by FFATA, and eSRS serves a separate purpose—i.e., it is an electronic system for reporting subcontracting plan compliance required by the Small Business Act.

SBA received several comments on redesignated § 125.3(c)(1)(viii) (former § 125.3(c)(1)(v)), which requires pre-award written notification to unsuccessful subcontractor offerors. SBA notes that this is not a new requirement (*see also* § 121.411(b)). SBA is only moving this provision as a result of amending this section to increase the subcontracting plan thresholds. One commenter argued that this rule creates an unnecessary administrative burden. The commenter noted that there is no specified tracking of compliance or listed consequence for failure to meet this requirement. SBA again notes that this notification is required by the current regulations. Further, this requirement is the only means to trigger any self-policing in the small business subcontracting community. The government may review compliance with this requirement as part of a compliance review.

Some commenters recommended clarifying the language: "for which a small business concern received a preference." One commenter noted that the FAR neither allows nor requires prime contractors to give small business preference on solicitations. Another commenter asked whether this language referred only to when a small business receives the award, or to all subcontracts set-aside for small businesses. This language is in the existing regulations and refers to subcontract competitions where consideration for award was limited based on size or socioeconomic status.

Use of Subcontractor in Performance

The proposed rule added new § 125.3(c)(3), providing that a prime contractor must represent that it will make a good faith effort to utilize the small business subcontractors used in preparing its bid or proposal during contract performance. SBA proposed that a prime contractor is deemed to have "used" a small business subcontractor in preparing its bid or proposal when: (i) The offeror specifically references a small business concern in a bid or proposal, (ii) the offeror has entered into a written agreement with the small business concern for purposes of performing the specific contract as a subcontractor, or (iii) the small business concern drafted portions of the proposal or submitted pricing or technical information that appears in the bid or proposal, with the intent or understanding that the small business concern will perform that related work if the offeror is awarded a contract. Some commenters opposed the provision in general terms, but as discussed previously, this provision is statutory and must be implemented. Some commenters requested clarifying whether this definition will be implemented in the FAR. SBA notes that this provision will be implemented in the FAR.

One commenter argued that "in the same amount and quality used in preparing and submitting the bid or proposal" is not feasible because quantities often change. SBA disagrees. This language is directly in the statute and is meant to address a specific problem. If the subcontractor was "used" in preparing the offer as defined in the regulation, then the prime contractor must provide the contracting officer with a written explanation as to why the subcontractor was not actually used in performance to the extent set forth in the offer. That explanation would certainly include any information relating to required quantities changing, so that the small business could not be used in performance to the same extent as that set forth in the offer.

One commenter noted that the proposed language would not address cases where a prime contractor issues a nominal subcontract but with significant down-scoping of the original

proposed work share, which according to the commenter is common practice. In response to this comment, SBA has amended § 125.3(c)(3) by adding the term "scope."

One commenter argued that commitments to suppliers are never made at time of proposal because an order may never be awarded, the supplier may go out of business, the supplier may be removed due to quality or delivery or other issues, or the supplier's quote may have expired before an award is received. The commenter argued that due to FAR competition requirements, many proposals are received and responded to which do not become actual orders. The commenter recommended that the government allow large businesses to place orders with small business concerns and reimburse them. As SBA stated in the proposed rule, responding to a request for a quote does not constitute use in preparing the bid or offer. SBA has added this language to § 125.3(c)(3). Further, the statute and regulation require the prime contractor to notify the contracting officer with an explanation, which could include all of those reasons (e.g., subcontractor out of business, quality or delivery issues, etc.).

Some commenters recommended requiring a more formal bid listing process requiring prime contractors to list in their bid the subcontractors they would use, allowing for later substitution if necessary. SBA considered requiring prime contractors to name subcontractors, but SBA has heard from the public and industry that selection of subcontractors in some industries does not occur until after contract award and requiring the prime to name subcontractors could result in a reduction of subcontracting opportunities.

Some commenters recommended requiring prime contractors to submit formal requests to amend subcontracting plans, arguing that this would assist in ensuring that prime contractors used the subcontractors named in their proposals. SBA disagrees. Subcontracting plans generally do not name specific small business concerns. Subcontracting plans simply establish goals for each socioeconomic category.

Some commenters recommended requiring prime contractors to include with their proposals fully executed subcontracts that are conditioned on the prime contractor's receipt of contract award and that are effective throughout the entire life of the contract. Other commenters recommended requiring a contract as evidence that a contractor failed to comply with proposed § 125.3(c)(3). SBA disagrees. In some industries, specific subcontracts are not solicited or awarded until well after contract award. Thus, it is not possible to impose a requirement that prime contractors include subcontracts in their proposals government-wide. At the same time, limiting the rule's applicability to situations where a formal subcontract has been executed would severely hamper the scope and breadth of the statutory provision. Further, it could have the effect of reducing prime contractors' willingness to enter into subcontracts prior to offer, which is clearly contrary to congressional intent.

One commenter argued that proposed § 125.3(c)(3) should not be triggered if a prime contractor awards the work to another small business and is otherwise not in violation of any contract by doing so. The commenter argued that the goal of the Jobs Act is to protect small business in general, not specific small businesses. SBA disagrees, and believes that the Jobs Act specifically intended to apply to and protect individual small businesses. This statutory provision does not reference whether or not the prime contractor is meeting its goals. The statute was intended to address the complaints of small businesses that expended significant time and resources to assist large businesses prepare bids, quotes and proposals that assisted those large businesses in being awarded a contract and then were not used in the performance of that contract.

One commenter suggested that the rule not apply if a quote from a small business is included in the bid or proposal as supporting documentation for a budget item. SBA disagrees. This is the type of behavior that the statute is intended to address. A prime contractor's inclusion of a quote in a bid raises the expectation of the subcontractor that its quote was used to win the award.

SBA received a number of comments recommending revisions to the language of proposed § 125.3(c)(3)(i)–(iii), which defined when an offeror used a small business in preparing a bid or proposal.

One commenter recommended revising § 125.3(c)(3)(i) to provide that an offeror used a small business concern in preparing the bid or proposal if "the offeror indicates it has awarded or selected the small business concern as a subcontractor to perform a portion of the specific contract." SBA disagrees. If the prime refers to the subcontractor in its proposal or bid in order to influence the award, that is precisely the conduct this statutory provision was intended to address, without limiting it to a further representation that a subcontract has been awarded. If the prime feels it is necessary to mention the subcontractor by name, the prime contractor must explain why that firm is not used in performance.

One commenter requested clarification of whether "bid or proposal" in § 125.3(c)(3)(i) includes small businesses listed in a subcontracting plan submitted with the bid or proposal. SBA has added language stating that "referenced in the bid or proposal" includes associated small business subcontracting plans, if applicable. SBA notes that subcontracting plans are not necessarily required at the time of bid or proposal and are often not required until the apparent successful offeror has been identified.

One commenter argued that proposed § 125.3(c)(3)(i) and (c)(3)(iii) are unduly broad, suggesting that it is the subcontractor's perception of future work, rather than a reasonable expectation on behalf of both parties, that triggers the rule's requirements. SBA disagrees and believes that the language of the proposed rule adequately captures the intent of the statute.

One commenter recommended defining the terms "agreement in principle" and "intent or understanding" in proposed § 125.3(c)(3)(ii). These terms will have to be interpreted by contracting officers and prime contractors on a case-by-case basis, as the provision is applied to specific factual circumstances.

One commenter recommended revising proposed § 125.3(c)(3)(ii) to read: "has a written agreement as to all material terms (including price, work scope, schedule, etc.) with the small business to perform as a subcontractor." As discussed in the proposed rule, the statute applies where the subcontractor was "used" in preparing the bid or proposal. Requiring the level of detail recommended by the commenter is not consistent with statutory intent.

One commenter recommended revising proposed § 125.3(c)(3)(ii) by replacing "agreement in principle" with "has made a written commitment to." SBA believes that "agreement in principle" is more consistent with statutory intent. Requiring written commitments might actually have the unintended effect of driving prime contractors to not enter into written agreements with subcontractors. Whether an agreement in principle existed will be a fact-specific exercise for the contracting officer to decide when evaluating prime contractor performance.

Some commenters recommended revising proposed § 125.3(c)(3)(iii) by replacing "intent or understanding" with a written communication standard. Commenters suggested that correspondence would be sufficient, and a signed contract would not be necessary. SBA concurs with this comment and has amended the regulation to clarify that evidence should be in writing.

The proposed rule added § 125.3(c)(4), which implemented Section 1322 of the Jobs Act. This provision established a requirement that a prime contractor on a covered contract must notify the contracting officer in writing if the prime contractor fails to utilize a small business concern used in preparing and submitting the prime contractor's bid or proposal.

SBA received eleven comments expressing concern that proposed § 125.3(c)(4) does not go far enough. Some commenters argued that prime contractors will not freely come forth and self-report. First, SBA notes that this notice requirement is statutory. In addition, SBA notes that the rule states that subcontractors can inform contracting officers of violations of this requirement.

Based on a comment, SBA has amended proposed § 125.3(c)(4) to state that the "prime contractor" rather than the "offeror" must provide the contracting officer with a written explanation as to why the prime did not acquire articles, equipment, supplies, services, or materials, or obtain the performance of construction work from the small business concerns that it used in preparing the bid or proposal, in the same scope, amount, and quality used in preparing and submitting the bid or proposal.

In addition, SBA has amended proposed § 125.3(c)(4) to clarify that the prime contractor must submit the written notification to the contracting officer prior to submitting to the Government the invoice for final payment and contract close-out.

One commenter suggested requiring prime contractors to inform subcontractors that subcontractors have the right to appeal to the contracting officer when the proposed small business is not used. SBA notes that the terms of the contract will determine the extent to which the contracting officer has control over who the prime contractor uses as a subcontractor. This statutory provision is intended only to include the prime contractor's utilization of subcontractors used in preparing the bid as part of the performance evaluation of the prime contractor.

One commenter recommended mirroring the requirement of DFAR 252.219–7003(g), arguing that lack of consistency between the rules will cause confusion. DFAR 252.219–7003(g) reads as follows: "In those subcontracting plans which specifically identify small businesses, the Contractor shall notify the Administrative Contracting Officer of any substitutions of firms that are not small business firms, for the small business firms specifically identified in the subcontracting plan. Notifications shall be in writing and shall occur within a reasonable period of time after award of the subcontract. Contractor-specified formats shall be acceptable." DFAR 252.219–7003(g) applies only when the prime contractor identifies specific small business concerns in the subcontracting plan, and no DFAR provision requires prime contractors to identify specific subcontractors in subcontracting plans. SBA believes that the language of the proposed rule more truly captures the statutory intent of this requirement. In any event, SBA's final rule will be implemented in the FAR and DFAR, and changes to those regulations will be made as necessary to ensure consistency.

One commenter asked whether the rule will apply retroactively. The general rule is that regulations apply to solicitations issued on or after the effective date of the regulation. However, this rule will have to be implemented in the FAR, and consideration will be given as to whether any of these provisions need to apply to existing contracts.

One commenter recommended requiring the prime contractor to report its intention not to use a designated subcontractor before the fact, rather than after the fact. Reporting is required if a subcontractor is not used in performance, and when that is triggered will depend on the specific facts and circumstances. The purpose of the reporting is primarily for purposes of evaluating the prime contractor's overall performance, and not necessarily for the purpose of affecting actual performance under the contract.

One commenter recommended prohibiting prime contractors from terminating subcontractors and then performing the work on their own. The commenter suggested requiring that small business subcontracts may only be terminated for cause, and the prime contractor must make a good faith effort to replace the subcontractor with another small business subcontractor, all of which is subject to the contracting officer's approval. In addition, the commenter suggested that if a small business subcontractor is acquired by a large firm, the prime contractor must replace the subcontractor with a new small business subcontractor within six months. These comments go well beyond statutory intent. The statute did not intend for the contracting officer to intercede in the private contractual relationships of commercial concerns.

One commenter recommended that the requirement should apply to all contracts. By statute, this requirement applies to all contracts requiring subcontracting plans. SBA believes that this was clear in the rule as proposed, and, as such, no further change is needed.

Some commenters opposed the requirement, arguing that suppliers are sometimes unable to fulfill requirements. SBA notes that this can be explained in the notice to the contracting officer.

Some commenters requested that SBA establish a threshold at which this reporting requirement would be triggered. Commenters also requested that SBA establish a timeframe for reporting. The statute does not create a threshold or a timeframe. SBA maintains that it will be incumbent upon the prime contractor to understand its subcontractors and proactively notify the contracting officer when the prime contractor has reason to believe that the relationship with the subcontractor met the definition. As for timeframe, it is difficult to set a timeframe because until the contract is completed, there is always theoretically a possibility that the prime contractor will use the subcontractor to the extent initially anticipated. Thus, it will be up to the prime contractor to come forward and notify the contracting officer when the prime contractor knows that the use of the subcontractor met the definition and that it will not use the subcontractor in performance in the same scope, amount, and quality as used in preparing and submitting the bid or proposal. However, SBA has added a requirement that the notice take place prior to submission of the final invoice for contract closeout.

Some commenters argued that the notification requirement will be a disincentive for prime contractors from specifically including small business concerns in their proposals, which limits small businesses' ability to participate in the development of proposals and gain valuable insight into how prime contractors approach proposals in general. SBA understands this concern, but the requirement is statutory. Obviously, small business subcontractors felt that statutory action was needed to address some prime

contractor mistreatment of some small business subcontractors.

Some commenters requested an exemption from the requirements in § 125.3(c)(4) and (c)(5) for non-profit research institutions, arguing that reporting and oversight were an onerous burden for these groups. In the alternative, one commenter recommended requiring such organizations to provide notice and justification only in annual reports. SBA does not adopt this comment. Nonprofits are not exempt under the statute and are not exempt from these reporting requirements.

Some commenters argued that contract awards attained via "bait & switch" should be vacated. SBA disagrees. In SBA's view, the intent was to use this information for purposes of evaluating performance. The statutory intent was not to require terminations whenever this provision was violated. Contracting officers have the discretion to consider such information for purposes of considering continued performance or exercising options, but SBA does not believe that mandating such action in all cases would be practical.

Late or Reduced Payment

The proposed rule added § 125.3(c)(5), which implemented Section 1334 of the Jobs Act. This provision established a requirement that a prime contractor notify the contracting officer in writing whenever a payment to a subcontractor is reduced or is 90 days or more past due for goods and services provided for the contract and for which the Federal agency has paid the contractor. SBA proposed that the prime contractor shall include the reason for the reduction in payment or failure to pay a subcontractor in the written notice.

SBA received over twenty comments on proposed § 125.3(c)(5). The commenters were split between those who suggested there be concrete consequences for prime contractors giving reduced or delayed payments, and those who argued that "unjustified" is not clearly defined, leaving prime contractors in a position to have to report in situations where the subcontractor is actually at fault.

In response to several comments, SBA has amended the language of § 125.3(c)(5) to clarify that this requirement applies only to small business subcontractors. The statutory provision pertains to contracts where a small business subcontracting plan is required, and such plans do not contain a goal for large business subcontractors.

Some commenters argued that the requirement should not apply when a prime contractor has attached only a quote for the purchase of goods or services in a bid, arguing that a quote is only a projection of cost and may change due to market conditions. In response to these comments, SBA has amended § 125.3(c)(5) to state that the reduced price applies only if the prime contractor awarded a subcontract.

One commenter suggested implementing a requirement similar to the requirement for agencies that are delinquent in reimbursing contractors. SBA notes that this information will be used for past performance evaluation purposes. A different statute governs payment to prime contractors.

One commenter recommended that the requirement should be extended to lower tier subcontractors that do not pay their subcontractors. SBA does not concur. The statute specifically refers to prime contractors and the contracting officer's ability to consider late payment in measuring prime contractor performance. There is lack of privity and authority between the government and lower tier subcontractors to extend the requirement as suggested.

Some commenters recommended that each invoice submitted by the prime contractor include a report of payments to be made to each subcontractor, listing the name of the subcontractor and the amount owed. SBA does not adopt this comment. This is not required by statute and would increase the recordkeeping and reporting requirements of prime contractors.

Some commenters opposed proposed § 125.3(c)(5) as too far-reaching. Some commenters argued that the requirement should apply only to late payments, not reduced payments. Other commenters recommended implementing the requirement on a contract-by-contract basis, based on the contracting officer's review of past performance. SBA does not concur. The statute specifically includes reduced payments and applies to all covered contracts.

Some commenters argued that federal construction contractors are already subject to more stringent requirements under the FAR, including sanctions under Title 18 of the United States Code for making false claims. SBA notes that the requirements that apply in the construction arena do not apply government-wide, while these provisions apply to all contracts. However, the more stringent construction requirements still apply.

Some commenters requested clarification of the definition of "unjustified" late or reduced payment. Some commenters suggested that the definition should not include situations where the prime contractor acted in good faith and pointed out that budget cuts, agency reorganization, and similar situations are common reasons for reduced payment. Some commenters argued that a prime contractor often has legitimate reasons (substandard performance, improper billing, performance of unauthorized work, etc.) for late or lower payment. One commenter recommended that SBA clarify that the reporting obligation should not apply if the late/reduced payment was the byproduct of a government change to requirements. One commenter recommended allowing prime contractors to appeal a determination that a reduction is "unjustified." SBA believes that the facts of a specific case should determine whether a late or reduced payment was justified or not. A prime contractor must communicate the reasons for making a late or reduced payment to the relevant contracting officer as part of its required notification. A contracting officer will then use his or her best judgment in determining whether the late or reduced payment was justified.

One commenter recommended clarifying what constitutes a "payment" to the prime contractor under different contract types. SBA notes that the opportunity for defining these terms will occur when these provisions are implemented in the FAR.

Some commenters suggested that reports be protected if they contain proprietary and/or classified information. One commenter recommended adding a provision that would exclude prime contractors from having to include in a report on the reasons for reduced or delayed payment where such information: (1) Is exempt from FOIA disclosure; (2) constitutes "contractor bid or proposal information" under the Procurement Integrity Act; or (3) is protected under the Privacy Act or other relevant law. SBA maintains that the reasons should be provided to the contracting officer—as required by statute—and the relevant information disclosure laws would apply to the reports. It is not up to prime contractors to interpret and apply information disclosure laws.

Some commenters requested clarification of "reduced price." In response to these comments, SBA has amended § 125.3(c)(5) to clarify that "reduced price" means the price is less than the amount initially agreed to in a written, binding contractual document.

Several commenters requested clarification of the term "upon completion of the responsibilities." Specifically, one commenter asked

whether the rule applies to payment reductions on progress payments. Another commenter asked whether the obligation of a contractor to report a reduced payment to a subcontractor applies to every payment made by the prime contractor or applies only at the completion of the entire subcontract. In response to these comments, SBA has amended § 125.3(c)(5) to state that the completion of responsibilities means that the subcontractor is entitled to payment under the terms of the subcontract.

Some commenters made recommendations for uniform payment terms for subcontracts. Such recommendations go beyond statutory intent and are beyond the scope of this rule.

One commenter recommended holding a public meeting where industry representatives from both large and small business may voice concerns. SBA held meetings in several cities to receive input on the proposed rule as part of its Jobs Act tour, and received significant written comments on the proposed rule. As such, SBA believes that additional public forums are unnecessary to fully understand the public concerns regarding the implementation of this rule. In addition, the public will have another opportunity to comment when this rule is incorporated in the FAR.

One commenter requested that SBA reduce the late payment definition from 90 days to 30 days. SBA does not adopt this comment. For purposes of this statutory reporting requirement, the statute defines late as being 90 days past due. This final rule continues to adopt the statutory definition.

One commenter recommended requiring agencies to publish actual payments to small business subcontractors. SBA does not adopt this comment. This requirement would be overly burdensome, and prime contractors as well as subcontractors may not want such information to be public. There is no clear public benefit from publicizing such information.

In response to comments, SBA has added new § 125.3(c)(6) to this final rule, which provides that if at the conclusion of a contract, the prime contractor did not meet all of the small business subcontracting goals in the subcontracting plan, the prime contractor shall provide the contracting officer with a written explanation as to why it did not meet the goals of the plan so that the contracting officer can evaluate whether the prime contractor acted in good faith as set forth in § 125.3(d)(3).

One commenter opposed proposed § 125.3(d)(5), arguing that payments to subcontractors may vary month to month under normal circumstances. The commenter also argued that subcontractors have existing legal means to receive payments due. Again, SBA notes that the requirement of proposed § 125.3(d)(5) is required by statute. In some circumstances, subcontractors do not have the resources to litigate claims, or may not want to exercise rights out of fear of not receiving future work.

One commenter recommended clarification of the differing language in proposed § 125.3(c)(5) ("more than 90 days past due") and proposed § 125.3(d)(5) ("more than 90 days late"). The commenter recommended changing both to "more than 90 days past the contractual due date." SBA has changed the language in both provisions to "90 days past due under the terms of the subcontract."

Contracting Officer Responsibilities

The proposed rule revised § 125.3(d) to clarify that the contracting officer is responsible for monitoring and evaluating the prime contractor's small business subcontracting plan compliance and reporting.

SBA received a number of comments expressing concern that over-extended contracting officers will not actually be able to monitor a prime contractor's compliance with the subcontracting plan on an ongoing basis as described in proposed § 125.3(d). SBA disagrees. Contracting officers are already required to monitor and evaluate prime contractors' compliance with subcontracting plans. The intent of this rule is simply to more clearly define the contracting officers' responsibilities.

Some commenters recommended Office of Small and Disadvantaged Business Utilization (OSDBU) participation in subcontracting plan compliance and enforcement. SBA disagrees. A subcontracting plan is a material part of a contract, and only the contracting officer has the authority to monitor contract performance. OSDBUs are not in the acquisition chain of command and have no authority to order a contracting officer to accept or reject a subcontracting plan or take some other enforcement action. Certainly, individual contracting officers may decide that OSDBUs can assist with subcontracting plan monitoring and enforcement, but SBA cannot impose a rule government-wide that gives OSDBUs authority over contracts.

Some commenters recommended requiring that the contracting officers in the field be responsible for monitoring compliance with subcontracting plans. SBA does not adopt this comment. The rule states the contracting officer is responsible, and if there is more than one contracting officer involved in a particular contract, the contracting agency must determine which contracting officer is responsible.

One commenter recommended the use of federal audit agencies to ensure that prime contractors comply with subcontracting requirements. Agencies may use audit agencies to assist in compliance, but SBA cannot mandate such a requirement in all cases. Audit agencies face resource challenges as well. SBA and the Defense Contract Management Agency (DCMA) do conduct subcontracting compliance reviews each year.

One commenter recommended requiring subcontracting program review once every two years if a prime contractor has active contracts with subcontracting plans. SBA does not adopt this comment. The contracting officer is responsible for reviewing, monitoring and evaluating a prime contractor's subcontracting plan performance with regard to each contract. In addition, compliance reviews conducted by SBA and DCMA occur as dictated by resource availability.

The proposed rule added new § 125.3(d)(1), which requires contracting officers to ensure that contractors submit their subcontracting reports into eSRS within 30 days after the report ending date. Some commenters recommended transparent monitoring to improve accountability of prime contractors. SBA notes that the eSRS system is a reporting system that enables a prime contractor to report to the contracting officer. Public access is beyond the scope of this rule, and access to the system is not controlled by SBA.

The proposed rule added § 125.3(d)(2), which requires the contracting officer to review every prime contractor's report within 60 days of the report ending date and accept or reject the report. One commenter recommended requiring contracting officers to give a reason for rejecting a report in order to ensure clarity and quick responses. SBA concurs and has amended proposed § 125.3(d)(2) to provide that the contracting officer should give an explanation for rejecting a report, since the eSRS system is already capable of doing this.

One commenter suggested that the language regarding conducting an SSR review should include "or designated Agency representative," arguing that

most agencies have an OSBP associate director review and accept SSRs, SBA recognizes that agencies usually have a person other than a contracting officer review the summary reports, since a summary report frequently contains achievements on multiple contracts with multiple contacting officers. However, the purpose of this rule is to clarify the responsibilities of the contracting officer.

One commenter recommended including language regarding the timeframe for a contracting officer to review all resubmitted reports. SBA notes that the same timeframes apply that apply to the submission of the original report.

The proposed rule amended redesignated § 125.3(d)(3) (former § 125.3(d)) to clarify that a contracting officer must evaluate whether a prime contractor made a good faith effort to comply with its small business subcontracting plan. The proposed rule maintained the current definition of when a prime contractor has made a good faith effort to comply with its small business subcontracting plan (redesignated § 125.3(d)(3)(i)–(iii), former § 125.3(d)(1)–(3)).

One commenter suggested that prime contractors that have not met subcontracting plan goals should be prohibited from receiving an option award until the prime contractor can show compliance. SBA disagrees. This could result in the government being deprived of vital goods or services and would severely hamper mission effectiveness.

Several commenters requested clarification of the actions contracting officers could take in response to a contractor's failure to meet its subcontracting goals. One commenter recommended that the government instruct contracting officers that compliance with a subcontract plan constitutes a material element of contract performance, with instruction to issue show cause notices and default terminations to prime contractors who fail to comply with subcontracting plans. SBA notes that the statute and the FAR provide that a subcontracting plan is a material part of a contract and provide for the possibility of liquidated damages, as well as the other actions noted by the commenter. However, these actions cannot be required by rule in all cases.

The proposed rule added new § 125.3(d)(4), which provides that the contracting officer must evaluate the prime contractor's written explanation concerning its failure to use a small business concern in the performance of a contract when that small business concern was used to prepare the bid or proposal.

One commenter recommended requiring the contracting officer to document a justification for awarding to a prime contractor with a history of not meeting subcontracting plan goals. SBA notes that contracting officers are required to consider subcontracting plan past performance in negotiated acquisitions. Further, SBA's regulations permit contracting officers to use other subcontracting-related evaluation factors.

SBA received significant negative comment on proposed § 125.3(d)(6), which provided that the contracting officer must consider whether to require a prime contractor to enter into a funds control agreement with a neutral third party if the prime contractor fails to pay subcontractors in a timely manner or fails to pay the agreed upon contractual price without justification. Although requested, SBA did not receive any comments explaining how this process should work or has worked in practice. Consequently, SBA has decided not to implement this provision in this final rule.

Proposed § 125.3(d)(7) required the contracting officer to record the identity of a prime contractor with a history of unjustified untimely payments to subcontractors in the Federal Awardee Performance and Integrity Information System (FAPIIS) or any successor system. This requirement is statutorily mandated. SBA received several comments supporting proposed § 125.3(d)(7) (changed to § 125.3(d)(6) in this final rule) but requesting that it go further in punishing non-compliant prime contractors. One commenter recommended a repository of names of prime contractors who have treated subcontractors poorly. SBA notes that the statutory requirement is FAPIIS.

One commenter asked whether these rules would override or interfere with already existing regulations concerning payment of subcontractors in the construction industry. These rules are in addition to, and do not supersede, other laws and regulations that apply to construction contracts, such as the requirement that the prime contractor certify in an invoice that all subcontractors have been paid or will be paid after payment. The commenter also asked whether information entered into FAPIIS concerning a prime contractor that has a history of unjustified late or reduced payment of subcontractors would be available to the public. That question is beyond the scope of this rule and SBA's knowledge. The commenter should inquire with GSA, the government agency responsible for FAPIIS.

The proposed rule added § 125.3(d)(8), providing that the contracting officer must require prime contractors to update their subcontracting plans whenever an option is exercised, as currently required by FAR 19.705–2(e). SBA received five comments expressing concerns that the additional reporting requirements at the time of option exercise would be burdensome.

One commenter argued that this requirement would be an administrative redundancy. The commenter argued that some agencies already call out for small business subcontracting plans to have subcontracting goals for individual option years. The commenter argued that there may be a lack of foreseeability when a contractor submits a proposal that a subcontracting plan may be required. The commenter argued that if a prime contractor is awarded an option continuing existing services, the prime contractor will already have subcontractors in place (mobilized and executing the work), which may not be small business concerns. The commenter argued that replacing the existing subcontractors would result in additional costs and operational inefficiency. SBA disagrees. The existing requirement in the FAR, which we are simply adding to SBA's regulations, requires the plan to be updated as necessary. All of the factors that the commenter articulates can be considered when deciding whether to change any of the percentages for an option period.

One commenter argued that if existing work is won through a recompete, then the new contract should have precedence over the old contract terms, subcontracting plan, personnel staffing, and other contract-related issues. SBA notes that new contracts should have new subcontracting plans, based on the subcontracting opportunities for the new contract.

One commenter argued that pursuant to FAR 19.704(c), a subcontracting plan is supposed to contain separate goals for the base contract and each option individually. The commenter argued that any updated subcontracting goals can be by a confirming correspondence and subsequent reporting. In the final rule, SBA has amended this provision (now contained in § 125.3(d)(7)) to state that the contracting officer has the discretion to require an updated subcontracting plan.

One commenter recommended that updates for options and modifications be considered as a new subcontracting requirement from the date of the

modification or the date the option is invoked, requiring a subcontracting plan only for the new portion of the work and only if that new work, standing alone, exceeds the applicable threshold. The commenter argued that this approach is consistent with FAR 19.702(a)(1). SBA has added a new § 125.3(d)(10) to clarify that the rule will apply to the subcontracting opportunities from that point forward and will not have retroactive effect. The ISR and SF–294 require that achievements be cumulative from the inception of the contract, and the accompanying instructions require that goals be rolled into the report as options are exercised. For example, if the base contract contained a small business goal of $10 million and each option contained a small business goal of $2 million, the small business goal for the entire contract in option year one would be $12 million. This ensures that the contracting officer is doing an "apples-to-apples" comparison when he compares achievements against goals.

SBA received six comments on proposed § 125.3(d)(9) (now § 125.3(d)(8)), under which the contracting officer must require a subcontracting plan if a modification causes the overall value of a contract to exceed the subcontracting plan threshold. As currently written, the FAR only requires a subcontracting plan if the value of the modification exceeds the subcontracting threshold. Commenters expressed concern about having to add a subcontracting plan if a modification to the contract raises the value above the subcontract threshold since this eventuality might occur when a substantial portion of the work has already been completed, and commitments have already been made on an ongoing basis. In response, SBA notes that plans are only required to the extent that subcontracting opportunities exist.

SBA received several comments on proposed § 125.3(d)(10) (now § 125.3(d)(9)), which allows a contracting officer to require a subcontracting plan if a prime contractor's size status changes from small to other than small as a result of a size recertification. Some commenters recommended requiring the contracting officer to require a subcontracting plan rather than making it discretionary. SBA disagrees. This is not required by statute. Further, it may be impractical to require a subcontracting plan at or near the end of performance, or after all subcontracting opportunities have passed. Thus, SBA maintains that it should be left to the discretion of the contracting officer.

Compliance Reviews

SBA received several comments addressing § 125.3(f) in general. One commenter recommended more third-party monitoring of prime contractors, with verification by affected subcontractors. SBA does not concur. Compliance with these provisions will be evaluated as part of the compliance reviews conducted by SBA, DCMA, Office of Naval Research, DLA Energy, and possibly other government agencies in the future; there are no other resources available. Another commenter recommended that contracting officers be required to respond to compliance review audits. SBA notes that a copy is sent to the contracting officer. Another commenter recommended that SBA perform more compliance reviews. SBA conducts as many as possible consistent with its resources and other priorities. One commenter argued that the compliance review requirements are potentially burdensome for prime contractors and difficult to obtain from other than small subcontractors. SBA disagrees. These requirements already exist. Without monitoring or spot checking, there is no incentive to properly administer subcontracting plans or to ensure that prime contractors are meeting their goals.

SBA received one comment on proposed § 125.3(f)(2)(i), which provided that a compliance review must include an analysis as to whether the prime contractor has assigned the correct NAICS code and corresponding size standard to the subcontract, and whether the subcontractor qualifies under the size or socioeconomic status claimed. The commenter recommended further clarification of proposed § 125.3(f)(2)(i). SBA notes that every subcontract must be assigned a NAICS code and size standard; otherwise there is no basis for a claim that a subcontract went to a small business. Thus, a compliance review must verify that that prime contractors or subcontractors are not improperly claiming to be small and using inappropriate NAICS codes and size standards.

SBA received several comments on proposed § 125.3(f)(2)(ii), which provided that a compliance review must include an analysis of whether the prime contractor is monitoring its other than small subcontractors with respect to their subcontracting plans, determining achievement of their subcontracting goals, and reviewing their ISRs or other reports.

Some commenters requested additional guidelines for monitoring. SBA notes that the prime contractor is responsible for making sure that the subcontracting plan requirements flow down to subcontractors and for monitoring subcontractor performance. Some commenters recommended clarifying the definition of the term "monitor." One commenter argued that prime contractors do not have the same abilities to do so with respect to subcontractors as the government does with respect to prime contractors. Whether or not prime contractors have the same ability to monitor performance of subcontractors as the government does for primes, the government has no ability to monitor a prime contractor's subcontractors. As such, this function must be the responsibility of prime contractors. SBA notes that this includes monitoring whether the relevant clauses are being included in subcontracts and whether goals are being met.

One commenter that opposed proposed § 125.3(f)(2)(iii) argued that prime contractors never before had to monitor other than small subcontractors' subcontracting plan compliance. This is incorrect. The FAR currently requires prime contractors to ensure that subcontractors issue subcontracting plans and issue reports.

Subcontracting Consideration in Source Selection

The proposed rule added new § 125.3(g)(1), under which SBA proposed to give agencies the discretion to consider subcontracting in source selection.

One commenter recommended that the FAR be amended to include subcontracting consideration in source selection. SBA notes that the rule will be implemented in the FAR after SBA's regulations are finalized.

SBA received six comments on proposed § 125.3(g)(1) requesting the inclusion of past prime contractor performance as an evaluation factor in source selection. SBA has agreed to amend its rule to make it clear that in addition to considering subcontracting plan compliance under a past performance factor, a contracting officer can also create an evaluation factor or subfactor specifically for purposes of considering subcontracting plan past performance.

One commenter recommended clarification of the circumstances under which the evaluation factor would apply. SBA notes that it applies only in full and open competition with value above the threshold, and it will apply at the discretion of the contracting officer.

One commenter recommended that government contractor past performance databases should be required to quantify successful compliance with

subcontracting plans. The commenter argued that this will assist source selection boards in determining the credibility of a concern's proposed subcontracting plan and past performance on a per-contract basis. SBA notes that like other aspects of the solicitation, the contracting officer will establish the parameters of the evaluation factor and what information should be submitted.

One commenter argued that this particular provision in the proposed rule will largely benefit small businesses that pursue contracts as Federal prime contractors and does not benefit (and in fact may have a detrimental impact on) small businesses that pursue work as Federal subcontractors. The commenter recommended an equivalent evaluation to assure that the awarded prime contractor—large or small—is providing maximum practicable opportunity to small business concerns at all levels of subcontracting. SBA disagrees. It is unclear how this proposal will harm small businesses. This proposal establishes an evaluation factor for small business subcontracting and ensures that a small business competing for a larger contract in full and open competition is not at a disadvantage, since small businesses are not required to have small business subcontracting plans. Small businesses will benefit either way—at the prime level or at the subcontracting level, depending on who wins the competition.

In response to several comments, SBA has redesignated proposed § 125.3(g)(2) (former § 125.3(g)) as § 125.3(g)(3) in this final rule and added a new paragraph (g)(2), providing that a contracting officer may include an evaluation factor in a solicitation which evaluates an other than small business concern's commitment to pay small business subcontractors within a specific number of days after receipt of payment from the Government.

Multi-agency, Federal Supply Schedule, Multiple Award Schedule and Governmentwide Acquisition IDIQ Contracts

The proposed rule added new § 125.3(h), which addresses subcontracting plans in connection with multiple award Multi-agency, Federal Supply Schedule, Multiple Award Schedule and Governmentwide acquisition indefinite delivery, indefinite quantity (IDIQ) contracts. Under proposed § 125.3(h)(1), SBA proposed that the contractor will report small business subcontracting achievement for individual orders to the contracting officer for the ordering or funding agency on an annual basis. SBA requested comments on whether the reporting requirement should apply to all orders or only apply to orders above a certain threshold.

SBA received eleven comments on proposed § 125.3(h)(1) expressing concerns that the additional reporting requirements for individual orders would be overly burdensome. Several commenters suggested creating a threshold level that would trigger the order-by-order reporting requirement. Some commenters recommended requiring reporting at the contract level or individual order level, but not both. Some commenters argued that the requirement should apply only to individual orders that are above a certain threshold. One commenter argued that on IDIQ contracts, a contractor may not know how many or which subcontractors are needed until the government issues task orders. Some commenters expressed concern about the additional burden imposed on large businesses or additional costs that might result from the requirement to report task-order subcontracting. Some commenters argued that contracting officers are already overburdened and that they should be spending time reviewing contracts rather than reports. One commenter who opposed the added reporting requirement argued that it is not required by statute. One commenter who supported the requirement recommended that all orders be reported with no minimum threshold to ensure maximum transparency.

Based on the comments received, SBA has decided that as a matter of policy the funding agency of an order should receive credit towards its small business subcontracting goals for orders awarded under another agency's contract. This policy is consistent with SBA's long-standing policy with respect to prime contracts, where the funding agency receives the credit towards its prime contracting goals for orders awarded under another agency's contract. The policy promotes transparency and accountability for prime contractors, and is consistent with the Small Business Jobs Act provisions concerning compliance, oversight and review of subcontracting plans. The requirement to report to the ordering agency on an annual basis will not be overly burdensome, as the new provision only applies where the funding agency and the contracting agency are not the same agency, and prime contractors already must report this information to the contracting agency. The contracting agency will still be responsible for the subcontracting plan for the underlying IDIQ contract. SBA recognizes that electronic reporting systems and the FAR will have to be revised before 125.3(i) can be implemented or utilized by ordering agencies or prime contractors. To ensure data integrity, SBA does make clear in this final rule that only one procuring agency may receive credit towards it subcontracting goals for a particular contracting action.

One commenter requested clarification regarding the applicability of proposed § 125.3(h)(1) to Blanket Purchase Agreements (BPAs) and Basic Ordering Agreements (BOAs). In the final rule, SBA has clarified that the contracting officer may establish subcontracting plans for BPAs and BOAs as well as orders. However, the annual reporting requirement for subcontracting credit purposes applies to orders issued under the BPA or BOA.

Compliance With Executive Orders 12866, 13563, 12988, 13132, the Paperwork Reduction Act (44 U.S.C. Ch. 35), and the Regulatory Flexibility Act (5. U.S.C. 601–612)

Executive Order 12866

The Office of Management and Budget (OMB) has determined that this final rule is a significant regulatory action for purposes of Executive Order 12866. Accordingly, the next section contains SBA's Regulatory Impact Analysis. This is not a major rule, however, under the Congressional Review Act, 5 U.S.C. 801, et seq.

Regulatory Impact Analysis

1. *Is there a need for the regulatory action?* The regulations implement Sections 1321, 1322 and 1334 of the Small Business Jobs Act of 2010, Public Law 111–240, 124 Stat. 2504, September 27, 2010 (Jobs Act); 15 U.S.C. 637(d)(6)(G), (d)(12). Section 1321 of the Jobs Act requires the Administrator to establish a policy on subcontracting compliance within one year of enactment.

2. *What are the potential benefits and costs of this regulatory action?* The regulations will benefit small business subcontractors by encouraging large business prime contractors to pay small business subcontractors in a timely manner and the agreed upon contractual price. The regulations will benefit small business subcontractors by encouraging large business contractors to utilize small business concerns in contract performance where the prime contractor used the small business concern to prepare the bid or proposal. The regulations will benefit small business subcontractors by clarifying the responsibilities of the contracting officer in monitoring small business

subcontracting plan compliance. The regulations will benefit small business subcontractors by specifically authorizing procuring agencies to consider proposed small business subcontracting when evaluating offers.

The regulations will benefit small business subcontractors by requiring large business concerns to report subcontracting results on an order-by-order basis, thereby enabling the funding agency to more closely monitor small business subcontracting in connection with the order and enabling the funding agency to receive credit towards its small business subcontracting goals. The regulation will benefit the contracting agency because the agency will not have to establish or monitor subcontracting plans for the contract. The rule benefits small business subcontractors by providing transparency with respect to small subcontracting on an order-by-order basis, thereby allowing the funding agency to monitor performance and establish subcontracting goals for particular orders.

eSRS will have to be altered to allow large business prime contractors to report subcontracting results on an order-by-order basis. Other systems may have to be altered to allow funding agencies to receive credit towards their small business subcontracting goals.

Large businesses will have to report to the contracting officer in writing when they fail to utilize a small business concern in contract performance when the prime contractor utilized the small business concern in preparing the bid or proposal. Large businesses will have to report to the contracting officer in writing when they fail to pay a subcontractor within 90 days or when they pay a subcontractor a reduced price. The contracting officer will have to consider these written explanations when evaluating contract performance. FAPIIS will have to be modified to allow contracting officers to identify large business prime contractors with a history of unjustified untimely payments.

3. *What are the alternatives to this final rule?* Many of the regulations set forth in this final rule are required to implement statutory provisions, and the Jobs Act requires promulgation of a policy on subcontracting compliance, a requirement that prime contractors notify the contracting officer when payment to a subcontractor is late, and a requirement that prime contractors notify the contracting officer when the prime contractor uses a subcontractor to prepare an offer but does not use the subcontractor in performance. The alternative to the regulation concerning orders would be to maintain the current environment, where subcontracting results are not reported on an order-by-order basis, and agencies funding orders do not receive credit towards their small business subcontracting goals.

Executive Order 13563

As part of its ongoing efforts to engage stakeholders in the development of its regulations, SBA solicited comments and suggestions from procuring agencies on how to best implement the Jobs Act. SBA held public forums around the country to discuss implementation of the Jobs Act. Where feasible, SBA incorporated public input into the rule. The regulations concerning evaluation factors provide contracting officers with the discretion to utilize various methods to improve small business subcontracting, without requiring their use in all cases. The rule concerning orders will provide contracting agencies with transparency by providing data concerning small business subcontracting for particular orders. Overall, these regulations minimize the burden resulting from these statutory provisions. SBA amended its regulations to remove outmoded thresholds that have increased and remove references to paper based forms that have been replaced by electronic reporting through eSRS.

As part of its implementation of this executive order and consistent with its commitment to public participation in the rulemaking process, SBA held public meetings in 13 locations around the country to discuss implementation of the Jobs Act, and received public input from thousands of small business owners, contracting officials and large business representatives. Although most of these amendments are new, SBA expects that public participation will help to form the Agency's retrospective analysis of related contracting regulations that are not being amended at this time.

Executive Order 12988

For purposes of Executive Order 12988, SBA has drafted this final rule, to the extent practicable, in accordance with the standards set forth in section 3(a) and 3(b)(2) of that Order, to minimize litigation, eliminate ambiguity, and reduce burden. This rule has no preemptive or retroactive effect.

Executive Order 13132

This rule does not have federalism implications as defined in Executive Order 13132. It will not have substantial direct effects on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various layers of government, as specified in the order. As such, it does not warrant the preparation of a Federalism Assessment.

Paperwork Reduction Act, 44 U.S.C. Ch. 35

For the purpose of the Paperwork Reduction Act, SBA has determined that this rule would impose new government-wide reporting requirements on large prime contractors. The Jobs Act requires such contractors to notify in writing contracting officers at the applicable procuring agency whenever a prime contractor fails to utilize a small business subcontractor used in preparing and submitting a bid or proposal; when the prime contractor pays a subcontractor a reduced price without justification; or when payments to a subcontractor are 90 days or more past due. These requirements will also be incorporated in the FAR.

Regulatory Flexibility Act, 5 U.S.C. 601–612

SBA has determined that this final rule may have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act (RFA), 5 U.S.C. 601–612. Therefore, SBA has prepared a Regulatory Flexibility Act (RFA) analysis addressing the regulatory provisions.

RFA

When preparing a Regulatory Flexibility Analysis, an agency shall address all of the following: a description of why the action by the agency is being considered; the objectives and legal basis of the rule; the estimated number of small entities to which the rule may apply; a description of the projected reporting, recordkeeping and other compliance requirements; identification of all Federal rules which may duplicate, overlap or conflict with the proposed rule; and a description of significant alternatives which minimize any significant economic impact on small entities. This RFA considers these points and the impact the proposed regulation concerning subcontracting may have on small entities.

(a) *Need for, Objectives, and Legal Basis of the Rule*

The majority of the regulatory amendments are required to implement Sections 1321, 1322 and 1334 of the Small Business Jobs Act of 2010, Public Law 111–240, 124 Stat. 2504, September 27, 2010 (Jobs Act); 15 U.S.C. 637(d)(6)(G), (d)(12). The regulations

that are not required by the Jobs Act are intended to help small business subcontractors by explicitly authorizing procuring agencies to consider proposed small business participation when evaluating offers from other than small business concerns. The regulations allow contracting officers to establish subcontracting plans and require other than small prime contractors to report data on small business subcontracting in connection with certain orders under existing contracts.

(b) *Estimate of the Number of Small Entities To Which the Rule May Apply*

The RFA directs agencies to provide a description of and, where feasible, an estimate of the number of entities that may be affected by the rules. The RFA defines "small entity" to include "small businesses," "small organizations," and "small governmental jurisdictions." SBA's programs generally do not apply to "small organizations" or "small governmental jurisdictions" because they are non-profit or governmental entities and do not generally qualify as "business concerns" within the meaning of SBA's regulations. SBA's programs generally apply only to for-profit business concerns. However, to the extent this rule will impact small organizations or small governmental jurisdictions that receive prime contracts from the Federal government with values that exceed the threshold, the numbers would be minimal, and the major provisions would only apply if the entity fails to pay or utilize small business subcontractors.

The final rule will not directly negatively affect any small business concern, because it applies to other than small concerns and contracting officers. The final rule will indirectly benefit small business concerns by requiring other than small prime contractors to report to the contracting officer when the prime contractor has failed to utilize a small business subcontractor used in preparing the bid or proposal. The final rule will also indirectly benefit small business concerns, by requiring large business prime contractors to report to the contracting officer when the prime contractor has failed to pay a small business subcontractor in a timely manner or pays a subcontractor a reduced rate without justification.

There are approximately 348,000 concerns listed as small business concerns in the Dynamic Small Business Search (DSBS) database. We do not know how many of these concerns participate in small business subcontracting. Firms do not need to register in the DSBS database to participate in subcontracting. The DSBS database is primarily used for prime contracting purposes. Thus, the number of firms participating in subcontracting may be greater than or lower than the number of firms registered in the DSBS database.

(c) *Projected Reporting, Recordkeeping and Other Compliance Requirements*

To the extent the rule imposes new information collection, recordkeeping or compliance requirements, these requirements are imposed on other than small business concerns, not on small business concerns.

(d) *Federal Rules Which May Duplicate, Overlap or Conflict With the Proposed Rule*

SBA is not aware of any rules which duplicate, overlap or conflict with the final rule. The final rule primarily implements statutory provisions.

(e) *Significant Alternatives to the Rule Which Could Minimize Impact on Small Entities*

Section 1321 of the Jobs Act requires SBA to promulgate regulations implementing it. Section 1321 of the Jobs Act and its implementing regulations primarily apply to contracting officers. Sections 1322 and 1334 of the Jobs Act amend portions of the Small Business Act, which SBA is responsible for administering and implementing through its regulations. The regulations implementing Sections 1322 and 1334 of the Jobs Act primarily apply to other than small concerns. As discussed above, the rule indirectly benefits small business concerns, without requiring small business concerns to report, keep records or take other compliance actions.

List of Subjects

13 CFR Part 121

Government procurement, Government property, Grant programs—business, Individuals with disabilities, Loan programs—business, Small businesses.

13 CFR Part 125

Government Contracting Programs; Small Business Subcontracting Program.

For the reasons set forth above, SBA amends parts 121 and 125 of title 13 of the Code of Federal Regulations as follows:

PART 121—SMALL BUSINESS SIZE REGULATIONS

■ 1. The authority citation for 13 CFR part 121 continues to read as follows:

Authority: 15 U.S.C. 632, 634(b)(6), 636(b), 662, and 694a(9).

■ 2. Amend § 121.404(g)(3)(ii) by adding the following sentence at the end of the paragraph:

121.404 When does SBA determine the size status of a business concern?

* * * * *

(g) * * *

(3) * * *

(ii) * * * However, a contracting officer may require a subcontracting plan if a prime contractor's size status changes from small to other than small as a result of a size recertification.

* * * * *

■ 3. Amend § 121.411 as follows:

■ a. Revise paragraph (a); and

■ b. Redesignate paragraphs (b) and (c) as paragraphs (c) and (d) and add new paragraph (b).

121.411 What are the size procedures for SBA's Section 8(d) Subcontracting Program?

(a) Prime contractors may rely on the information contained in the System for Award Management (SAM) (or any successor system or equivalent database maintained or sanctioned by SBA) as an accurate representation of a concern's size and ownership characteristics for purposes of maintaining a small business source list.

(b) Even if a concern is on a small business source list, it must still qualify and self-certify as a small business at the time it submits its offer as a section 8(d) subcontractor. Prime contractors may accept a subcontractor's electronic self-certifications as to size, if the subcontract contains a clause which provides that the subcontractor verifies by submission of the offer that the size or socioeconomic representations and certifications made in SAM (or any successor system) are current, accurate and complete as of the date of the offer for the subcontract. Prime contractors or subcontractors may not require the use of SAM (or any successor system) for purposes of representing size or socioeconomic status in connection with a subcontract.

* * * * *

PART 125—GOVERNMENT CONTRACTING PROGRAMS

■ 4. The authority citation for part 125 is revised to read as follows:

Authority: 15 U.S.C. 632(p), (q); 634(b)(6); 637; 644 and 657(f); Pub. L. 111–240, § 1321.

■ 5. Amend § 125.3 as follows:

■ a. Revise paragraph (a);

■ c. Revise paragraphs (b)(1) and (b)(3)(ii);

■ d. Revise paragraph (c)(1) introductory text;

■ e. Revise paragraphs (c)(1)(iii)–(vi);

■ f. Add new paragraphs (c)(1)(vii)–(ix);
■ g. Redesignate paragraph (c)(3) as (c)(7) and add new paragraphs (c)(3), (c)(4), (c)(5) and (c)(6);
■ h. Revise paragraph (d);
■ i. Revise paragraph (e)(3);
■ j. Revise paragraphs (f)(1) and (f)(2);
■ k. Revise paragraph (g); and
■ l. Add new paragraph (h).

§ 125.3 Subcontracting assistance.

(a) *General.* The purpose of the subcontracting assistance program is to provide the maximum practicable subcontracting opportunities for small business concerns, including small business concerns owned and controlled by veterans, small business concerns owned and controlled by service-disabled veterans, certified HUBZone small business concerns, certified small business concerns owned and controlled by socially and economically disadvantaged individuals, and small business concerns owned and controlled by women. The subcontracting assistance program implements section 8(d) of the Small Business Act, which includes the requirement that, unless otherwise exempt, other than small business concerns awarded contracts that offer subcontracting possibilities by the Federal Government in excess of $650,000, or in excess of $1,500,000 for construction of a public facility, must submit a subcontracting plan to the appropriate contracting agency. The Federal Acquisition Regulation sets forth the requirements for subcontracting plans in 48 CFR 19.7, and the clause at 48 CFR 52.219–9.

(1) Subcontract under this section means any agreement (other than one involving an employer-employee relationship) entered into by a Government prime contractor or subcontractor calling for supplies and/or services required for performance of the contract or subcontract (including modifications).

(i) Subcontract award data reported by prime contractors and subcontractors shall be limited to awards made to their immediate next-tier subcontractors. Credit cannot be taken for awards made beyond the immediate next-tier, except as follows:

(A) The contractor or subcontractor has been designated to receive a small business or small disadvantaged business credit from an ANC or Indian Tribe; or

(B) Purchases from a corporation, company, or subdivision that is an affiliate of the prime contractor or subcontractor are not included in the subcontracting base. Subcontracts by first-tier affiliates shall be treated as subcontracts of the prime.

(ii) Only subcontracts involving performance in the United States or its outlying areas should be included, with the exception of subcontracts under a contract awarded by the U.S. Department of State or any other agency that has statutory or regulatory authority to require subcontracting plans for subcontracts performed outside the United States and its outlying areas and subcontracts for foreign military sales unless waived in accordance with agency regulations.

(iii) The following should not be included in the subcontracting base: internally generated costs such as salaries and wages; employee insurance; other employee benefits; payments for petty cash; depreciation; interest; income taxes; property taxes; lease payments; bank fees; fines, claims, and dues; Original Equipment Manufacturer relationships during warranty periods (negotiated up front with product); utilities such as electricity, water, sewer, and other services purchased from a municipality or solely authorized by the municipality to provide those services in a particular geographical region; and philanthropic contributions. Utility companies may be eligible for additional exclusions unique to their industry, which may be approved by the contracting officer on a case-by-case basis. Exclusions from the subcontracting base include but are not limited to those listed above.

(2) Subcontracting goals required under paragraph (c) of this section must be established in terms of the total dollars subcontracted and as a percentage of total subcontract dollars. However, a contracting officer may establish additional goals as a percentage of total contract dollars.

(3) A prime contractor has a history of unjustified untimely or reduced payments to subcontractors if the prime contractor has reported itself to a contracting officer in accordance with paragraph (c)(5) of this section on three occasions within a 12 month period.

(b) *Responsibilities of prime contractors.* (1) Prime contractors (including small business prime contractors) selected to receive a Federal contract that exceeds the simplified acquisition threshold, that will not be performed entirely outside of any state, territory, or possession of the United States, the District of Columbia, or the Commonwealth of Puerto Rico, and that is not for services which are personal in nature, are responsible for ensuring that small business concerns have the maximum practicable opportunity to participate in the performance of the contract, including subcontracts for subsystems, assemblies, components, and related services for major systems, consistent with the efficient performance of the contract.

* * * * *

(3) * * *

(ii) Conducting market research to identify small business subcontractors and suppliers through all reasonable means, such as performing online searches via the System for Award Management (SAM) (or any successor system), posting Notices of Sources Sought and/or Requests for Proposal on SBA's SUB-Net, participating in Business Matchmaking events, and attending pre-bid conferences;

* * * * *

(c) *Additional responsibilities of large prime contractors.* (1) In addition to the responsibilities provided in paragraph (b) of this section, a prime contractor selected for award of a contract or contract modification that exceeds $650,000, or $1,500,000 in the case of construction of a public facility, is responsible for the following:

* * * * *

(iii) The contractor may not prohibit a subcontractor from discussing any material matter pertaining to payment or utilization with the contracting officer;

(iv) When developing an individual subcontracting plan (also called individual contract plan), the contractor must decide whether to include indirect costs in its subcontracting goals. If indirect costs are included in the goals, these costs must be included in the Individual Subcontract Report (ISR) in www.esrs.gov (eSRS) or Subcontract Reports for Individual Contracts (the paper SF–294, if authorized). If indirect costs are excluded from the goals, these costs must be excluded from the ISRs (or SF–294 if authorized); however, these costs must be included on a prorated basis in the Summary Subcontracting Report (SSR) in the eSRS system. A contractor authorized to use a commercial subcontracting plan must include all indirect costs in its SSR;

(v) The contractor must assign each subcontract the NAICS code and corresponding size standard that best describes the principal purpose of the subcontract (*see* § 121.410). The prime contractor may rely on subcontractor self-certifications made in SAM (or any successor system), if the subcontract contains a clause which provides that the subcontractor verifies by submission of the offer that the size or socioeconomic representations and certifications in SAM (or any successor system) are current, accurate and

complete as of the date of the offer for the subcontract. A prime contractor or subcontractor may not require the use of SAM (or any successor system) for purposes of representing size or socioeconomic status in connection with a subcontract;

(vi) The contractor must submit timely and accurate ISRs and SSRs in eSRS (or any successor system), or if information for a particular procurement cannot be entered into eSRS (or any successor system), submit a timely SF–294, Subcontracting Report for Individual Contract. When a report is rejected by the contracting officer, the contractor must make the necessary corrections and resubmit the report within 30 days of receiving the notice of rejection;

(vii) The contractor must cooperate in the reviews of subcontracting plan compliance, including providing requested information and supporting documentation reflecting actual achievements and good-faith efforts to meet the goals and other elements in the subcontracting plan;

(viii) The contractor must provide pre-award written notification to unsuccessful small business offerors on all subcontracts over $150,000 for which a small business concern received a preference. The written notification must include the name and location of the apparent successful offeror and if the successful offeror is a small business, veteran-owned small business, service-disabled veteran-owned small business, HUBZone small business, small disadvantaged business, or women-owned small business; and

(ix) As a best practice, the contractor may provide the pre-award written notification cited in paragraph (c)(1)(viii) of this section to unsuccessful and small business offerors on subcontracts at or below $150,000 and should do so whenever practical.

* * * * *

(3) An offeror must represent to the contracting officer that it will make a good faith effort to acquire articles, equipment, supplies, services, or materials, or obtain the performance of construction work from the small business concerns that it used in preparing the bid or proposal, in the same scope, amount, and quality used in preparing and submitting the bid or proposal. Merely responding to a request for a quote does not constitute use in preparing a bid or offer. An offeror used a small business concern in preparing the bid or proposal if:

(i) The offeror references the small business concern as a subcontractor in the bid or proposal or associated small business subcontracting plan;

(ii) The offeror has a subcontract or agreement in principle to subcontract with the small business concern to perform a portion of the specific contract; or

(iii) The small business concern drafted any portion of the bid or proposal or the offeror used the small business concern's pricing or cost information or technical expertise in preparing the bid or proposal, where there is written evidence (including email) of an intent or understanding that the small business concern will be awarded a subcontract for the related work if the offeror is awarded the contract.

(4) If a prime contractor fails to acquire articles, equipment, supplies, services or materials or obtain the performance of construction work as described in (c)(3), the prime contractor must provide the contracting officer with a written explanation. This written explanation must be submitted to the contracting officer prior to the submission of the invoice for final payment and contract close-out.

(5) A prime contractor shall notify the contracting officer in writing if upon completion of the responsibilities of the small business subcontractor (i.e., the subcontractor is entitled to payment under the terms of the subcontract), the prime contractor pays a reduced price to a small business subcontractor for goods and services provided for the contract or the payment to a small business subcontractor is more than 90 days past due under the terms of the subcontract for goods and services provided for the contract and for which the Federal agency has paid the prime contractor. "Reduced price" means a price that is less than the price agreed upon in a written, binding contractual document. The prime contractor shall include the reason for the reduction in payment to or failure to pay a small business subcontractor in any written notice.

(6) If at the conclusion of a contract the prime contractor did not meet all of the small business subcontracting goals in the subcontracting plan, the prime contractor shall provide the contracting officer with a written explanation as to why it did not meet the goals of the plan so that the contracting officer can evaluate whether the prime contractor acted in good faith as set forth in paragraph (d)(3) of this section.

(d) *Contracting officer responsibilities.* The contracting officer (or administrative contracting officer if specifically delegated in writing to accomplish this task) is responsible for evaluating the prime contractor's compliance with its subcontracting plan, including:

(1) Ensuring that all contractors submit their subcontracting reports into the eSRS (or any successor system) or, if applicable, the SF–294, Subcontracting Report for Individual Contracts, within 30 days after the report ending date (e.g., by October 30th for the fiscal year ended September 30th).

(2) Reviewing all ISRs, and where applicable, SSRs, in eSRS (or any successor system) within 60 days of the report ending date (e.g., by November 30th for a report submitted for the fiscal year ended September 30th) and either accepting or rejecting the reports in accordance with the Federal Acquisition Regulation (FAR) provisions set forth in 48 CFR subpart 19.7, 52.219–9, and the eSRS instructions (www.esrs.gov). The authority to acknowledge or reject SSRs for commercial plans resides with the contracting officer who approved the commercial plan. If a report is rejected, the contracting officer must provide an explanation for the rejection to allow prime contractors the opportunity to respond specifically to perceived deficiencies.

(3) Evaluating whether the prime contractor made a good faith effort to comply with its small business subcontracting plan. Evidence that a large business prime contractor has made a good faith effort to comply with its subcontracting plan or other subcontracting responsibilities includes supporting documentation that:

(i) The contractor performed one or more of the actions described in paragraph (b) of this section, as appropriate for the procurement;

(ii) Although the contractor may have failed to achieve its goal in one socioeconomic category, it over-achieved its goal by an equal or greater amount in one or more of the other categories; or

(iii) The contractor fulfilled all of the requirements of its subcontracting plan.

(4) Evaluating the prime contractor's written explanation concerning the prime contractor's failure to use a small business concern in performance in the same scope, amount, and quality used in preparing and submitting the bid or proposal, and considering that information when rating the contractor for past performance purposes.

(5) Evaluating the prime contractor's written explanation concerning its payment of a reduced price to a small business subcontractor for goods and services upon completion of the responsibilities of the subcontractor or its payment to a subcontractor more than 90 days past due under the terms

of the subcontract for goods and services provided for the contract and for which the Federal agency has paid the prime contractor, and considering that information when rating the contractor for past performance purposes.

(6) Evaluating whether the prime contractor has a history of unjustified untimely or reduced payments to subcontractors, and if so, recording the identity of the prime contractor in the Federal Awardee Performance and Integrity Information System (FAPIIS), or any successor database.

(7) In his or her discretion, requiring the prime contractor (other than a prime contractor with a commercial plan) to update its subcontracting plan when an option is exercised.

(8) Requiring the prime contractor (other than a contractor with a commercial plan) to submit a subcontracting plan if the value of a modification causes the value of the contract to exceed the subcontracting plan threshold and to the extent that subcontracting opportunities exist.

(9) In his or her discretion, requiring a subcontracting plan if a prime contractor's size status changes from small to other than small as a result of a size recertification.

(10) Where a subcontracting plan is amended in connection with an option, or added as a result of a recertification or modification, the changes to any existing plan are for prospective subcontracting opportunities and do not apply retroactively. However, since achievements must be reported on the ISR (or the SF–294, if applicable) on a cumulative basis from the inception of the contract, the contractor's achievements prior to the modification or option will be factored into its overall achievement on the contract from inception.

(e) * * *

(3) Instructing large prime contractors on identifying small business concerns by means of SAM (or any successor system), SUB-Net, Business Matchmaking events, and other resources and tools;

* * * * *

(f) *Compliance reviews.* (1) A prime contractor's performance under its subcontracting plan is evaluated by means of on-site compliance reviews and follow-up reviews. A compliance review is a surveillance review that determines a contractor's achievements in meeting the goals and other elements in its subcontracting plan for both open contracts and contracts completed during the previous twelve months. A follow-up review is done after a compliance review, generally within six to eight months, to determine if the contractor has implemented SBA's recommendations.

(2) All compliance reviews begin with a validation of the prime contractor's most recent ISR (or SF–294, if applicable) or SSR. A compliance review includes:

(i) An evaluation of whether the prime contractor assigned the proper NAICS code and corresponding size standard to a subcontract, and a review of whether small business subcontractors qualify for the size or socioeconomic status claimed;

(ii) Validation of the prime contractor's methodology for completing its subcontracting reports; and

(iii) Consideration of whether the prime contractor is monitoring its other than small subcontractors with regard to their subcontracting plans, determining achievement of their proposed subcontracting goals, and reviewing their subcontractors' ISRs (or SF–294s, if applicable).

* * * * *

(g) *Subcontracting consideration in source selection.* (1) A contracting officer may include an evaluation factor in a solicitation which evaluates:

(i) An offeror's proposed approach to small business subcontracting participation in the subject procurement;

(ii) The extent to which the offeror has met its small business subcontracting plan goals on previous covered contracts; and/or

(iii) The extent to which the offeror timely paid its small business subcontractors under covered contracts.

(2) A contracting officer may include an evaluation factor in a solicitation which evaluates an offeror's commitment to pay small business subcontractors within a specific number of days after receipt of payment from the Government for goods and services previously rendered by the small business subcontractor.

(i) The contracting officer will comparatively evaluate the proposed timelines.

(ii) Such a commitment shall become a material part of the contract.

(iii) The contracting officer must consider the contractor's compliance with the commitment in evaluating performance, including for purposes of contract continuation (such as exercising options).

(3) A small business concern submitting an offer shall receive the maximum score, credit or rating under an evaluation factor described in paragraph (g) of this section without having to submit any information in connection with this factor.

(4) A contracting officer shall include a significant evaluation factor for the criteria described in paragraphs (g)(2)(i) and (g)(2)(ii) of this section in a bundled contract or order as defined in § 125.2.

(5) Paragraph (g) of this section may apply to solicitations for orders against multiple award contracts, (including a Federal Supply Schedule or Multiple Award Schedule contract, a Government-wide acquisition contract (GWAC), or a multi-agency contract (MAC)), blanket purchase agreements or basic ordering agreements.

(h) *Multiple award contracts.* (1) Except where a prime contractor has a commercial plan, the contracting officer shall require a subcontracting plan for each multiple award indefinite delivery, indefinite quantity contract (including Multiple Award Schedule), where the estimated value of the contract exceeds the subcontracting plan thresholds in paragraph (a) of this section and the contract has subcontracting opportunities.

(2) Contractors shall submit small business subcontracting reports for individual orders to the contracting agency on an annual basis.

(3) The agency funding the order shall receive credit towards its small business subcontracting goals. More than one agency may not receive credit towards its subcontracting goals for a particular subcontract.

(4) The agency funding the order may in its discretion establish small business subcontracting goals for individual orders, blanket purchase agreements or basic ordering agreements.

Dated: June 25, 2013.

Karen G. Mills,

Administrator.

[FR Doc. 2013–16967 Filed 7–15–13; 8:45 am]

BILLING CODE 8025–01–P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 39

[Docket No. FAA–2013–0522; Directorate Identifier 2013–SW–018–AD; Amendment 39–17487; AD 2013–10–51]

RIN 2120–AA64

Airworthiness Directives; Eurocopter France Helicopters

AGENCY: Federal Aviation Administration (FAA), Department of Transportation (DOT).

ACTION: Final rule; request for comments.

Exhibit 2:

Size and Status Integrity, 78 Fed. Reg. 38811, June 28, 2013

Rules and Regulations

Federal Register
Vol. 78, No. 125
Friday, June 28, 2013

This section of the FEDERAL REGISTER contains regulatory documents having general applicability and legal effect, most of which are keyed to and codified in the Code of Federal Regulations, which is published under 50 titles pursuant to 44 U.S.C. 1510.

The Code of Federal Regulations is sold by the Superintendent of Documents. Prices of new books are listed in the first FEDERAL REGISTER issue of each week.

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

6 CFR Part 1000

[PCLOB; Docket No. 2013–0005; Sequence 2]

RIN 0311–AA02

Organization and Delegation of Powers and Duties; Correction

AGENCY: Privacy and Civil Liberties Oversight Board.

ACTION: Final rule; correction.

SUMMARY: The Privacy and Civil Liberties Oversight Board is issuing a correction to fix a duplicate section designation published in a final rule in the **Federal Register** on June 5, 2013.

DATES: This correction is effective June 28, 2013.

FOR FURTHER INFORMATION CONTACT: Susan Reingold, Chief Administrative Officer, Privacy and Civil Liberties Oversight Board, at 202–331–1986.

SUPPLEMENTARY INFORMATION:

Correction

In rule FR Doc. 2013–13166 published in the **Federal Register** at 78 FR 33690, June 5, 2013, an incorrect section heading was codified.

Accordingly, the Privacy and Civil Liberties Oversight Board amends 6 CFR part 1000 by making the following correcting amendment:

PART 1000—ORGANIZATION AND DELEGATION OF POWERS AND DUTIES OF THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

■ 1. The authority citation for part 1000 continues to read as follows:

Authority: 5 U.S.C. 552.

§ 1000.3 Corrected.

■ 2. The second and erroneous occurrence of § 1000.3 (Delegations of authority) is correctly redesignated as § 1000.5.

Dated: June 24, 2013.

Diane M. Janosek,

Chief Legal Counsel.

[FR Doc. 2013–15536 Filed 6–27–13; 8:45 am]

BILLING CODE 6820–B3–P

SMALL BUSINESS ADMINISTRATION

13 CFR Parts 121, 124, 125, 126, and 127

RIN 3245–AG23

Small Business Size and Status Integrity

AGENCY: Small Business Administration.

ACTION: Final rule.

SUMMARY: This rule implements provisions of the Small Business Jobs Act of 2010 (Jobs Act) pertaining to small business size and status integrity. This rule amends the U.S. Small Business Administration's (SBA or Agency) program regulations to implement statutory provisions establishing that there a presumption of loss equal to the value of the contract or other instrument when a concern willfully seeks and receives an award by misrepresentation. The rule implements statutory provisions that provide that: The submission of an offer or application for an award intended for small business concerns will be deemed a size or status certification or representation in certain circumstances; an authorized official must sign in connection with a size or status certification or representation for a contract or other instrument; and concerns that fail to update their size or status in the Online Representations and Certifications Application (ORCA) database or a successor thereto (such as the System for Award Management (SAM) database) at least annually shall no longer be identified in the database as small or some other socioeconomic status, until the representation is updated. The rule also amends SBA's regulations to clarify when size is determined for purposes of entry into the 8(a) Business Development, HUBZone and Small Disadvantaged Business (SDB) programs.

DATES: This rule is effective August 27, 2013.

FOR FURTHER INFORMATION CONTACT: Dean R. Koppel, Office of Government Contracting, 409 Third Street SW., Washington, DC 20416; (202) 205–7322; *dean.koppel@sba.gov.*

SUPPLEMENTARY INFORMATION: On September 27, 2010, Congress amended the Small Business Act to provide that if a concern willfully seeks and receives an award by misrepresenting its small business size or status, there is a presumption of loss to the United States equal to the value of the contract, subcontract, cooperative agreement, cooperative research and development agreement or grant. The Small Business Act was also amended to provide that certain actions, such as submitting an offer in response to a solicitation set aside for small business concerns, will be deemed a representation of small business size or status. The Small Business Act was amended to provide that the signature of an authorized official of a concern is required in making a small business size or status representation in connection with certain actions, such as submitting an offer. The Small Business Act now provides that concerns must update their size and status certifications in SAM at least annually, or the status will be lost until such time as the update is made. Finally, the Small Business Act provides that SBA must promulgate regulations to protect individuals and concerns from liability in cases of unintentional errors, technical malfunctions and other similar situations.

SBA published a proposed rule regarding these statutory provisions in the **Federal Register** on October 7, 2011 (76 FR 62313), inviting the public to submit comments on or before November 7, 2011. This comment period was extended through December 8, 2011 by notice in the **Federal Register** published on November 8, 2011 (76 FR 69154).

Summary of Comments and SBA's Responses

SBA received and considered twenty comments on the proposed rule. Two commenters fully supported the rule as proposed. One comment addressed the proposed Small Business Subcontracting Rule published at 76 FR 61626 on October 5, 2011. This comment was outside the scope of this proposed rulemaking and was not

considered in adopting this final rule. The remaining comments, as well as SBA's response to them, are discussed below.

Presumption of Loss

SBA received several comments regarding SBA's proposal that the presumption of loss to the United States for a willful misrepresentation of size or status be irrefutable. 13 CFR §§ 121.108(a), 121.411(d), 124.521(a), 124.1015(a), 125.29(a), 126.900(a), and 127.700(a). As noted in the proposed rule, SBA based its proposed imposition of an irrefutable presumption of loss on Senate Report language indicating that the presumption shall be "irrefutable." Senate Rep. No. 111–343, p. 8, available at: *http://www.gpo.gov.*

One commenter suggested that SBA eliminate "irrefutable" from the regulatory text. This commenter stressed that: (1) Irrefutable presumptions deny due process of law; and (2) Senate Report language does not possess statutory authority. Another commenter argued that the cited Senate Report was not the Senate Report for the legislation in question, but was instead a Senate Report for a prior piece of proposed legislation. Upon additional reflection, SBA has decided to remove the term "irrefutable" from the regulations, rendering the presumption rebuttable. SBA notes that the presumption of loss provisions will be utilized in civil and criminal Federal court proceedings, where due process will be provided. Further, SBA's regulations limit liability in the case of unintentional error, technical malfunction, or other similar situations. 13 CFR §§ 121.108(d), 121.411(g), 124.521(d), 124.1015(d), 125.29(d), 126.900(d), and 127.700(d). As such, an "irrefutable" presumption would be inappropriate in these instances.

Another commenter suggested that SBA ensure firms have sufficient due process to contest a finding of willful misrepresentation before penalties are imposed. This commenter made several suggestions as to how SBA could ensure protection of business concerns' due process—these suggestions included: (1) Provision of an agency level response period; and (2) empowering SBA's Office of Hearings and Appeals (OHA) to hear appeals of determinations under the proposed rule. As discussed above, the statutory presumption of loss provisions will be applied in Federal civil and criminal court proceedings where due process will be provided and as explained above, in certain instances, SBA's regulations limit liability. 13 CFR §§ 121.108(d), 121.411(g), 124.521(d), 124.1015(d), 125.29(d), 126.900(d), and 127.700(d). As such, SBA does not believe that this provision requires modification.

One commenter suggested that SBA impose a rebuttable presumption where a size determination finds that a firm is small by itself (i.e., absent the firm's affiliates) that the firm did not willfully misrepresent its size. Likewise, this commenter suggested that SBA impose a rebuttable presumption that the firm willfully misrepresented its size when a size determination finds the firm to be other than small by itself (i.e., absent the firm's affiliates). As discussed above, the rule now provides that the presumption is rebuttable. The question of whether a firm has willfully misrepresented its size is a factual determination best made by a judge, jury, or other decider of fact. Given the fact-specific nature of such a finding, SBA declines to impose a presumption as to an actor's intent.

Two commenters suggested clarification of the language in proposed 13 CFR §§ 121.108(a), 121.411(d), 124.521(a), 124.1015(a), 125.29(a), 126.900(a), and 127.700(a) which provide that the presumption of loss applies "whenever it is established" that a firm willfully misrepresented its status. Specifically, the commenters requested clarification of who makes the finding of willful misrepresentation, how a firm is notified of such a finding, whether the determination is appealable, and how a company may defend its representation. Consistent with the intent of the Jobs Act, it is SBA's intent that the presumption of loss shall be applied in all manner of criminal, civil, administrative, contractual, common law, or other actions, which the United States government may take to redress willful misrepresentation. As such, the finder of fact, notice requirements, and means of defense must depend on the specific action taken against a business concern. SBA does not believe any changes to the proposed rule or other clarification would be appropriate and adopts the proposed provisions as final in this rule.

Another commenter requested clarification as to whether an adverse size determination automatically leads to a presumption that the relevant firm willfully misrepresented its size. SBA recognizes that an unsophisticated firm or one new to the Federal government arena may certify its status as a small business in good faith, but may ultimately be found to be other than small. Similarly, a firm may incorrectly apply an ownership or control requirement for the service-disabled veteran-owned (SDVO) or women-owned small business (WOSB) programs in good faith, and ultimately be found not to qualify as a SDVO or WOSB small business. In either case, if the situation truly is a good faith misinterpretation of SBA's rules, SBA does not believe that action should be taken against the firm or its principals. Again, the question of whether a firm submitted a misrepresentation in good faith or intentionally (or recklessly) submitted a false size or status representation or certification is a factual determination best made by a judge, jury, or other decider of fact.

One commenter recommended that SBA amend the proposed rule to include a provision requiring the government to "prominently mark" any solicitation set aside as contemplated by the proposed rule. Currently, solicitations issued under the Federal Acquisition Regulation (FAR) must contain specific clauses providing notice regarding set-asides, reserves, partial set-asides, price evaluation preferences, source selection factors, and other mechanisms which somehow classify a solicitation as intended for award to specific entities. 48 CFR §§ 52.219–3, 52.219–4, 52.219–6, 52.219–7, 52.219–13, 52.219–18, 52.219–23, 52.219–27, 52.219–29, and 52.219–30. Therefore, SBA does not believe any change to the rule is necessary.

One commenter requested clarification of situations where an offer may be "otherwise classified as intended for award to small business" without being specifically identified as set aside for small business. Consistent with the underlying statutory text, it is SBA's intent that the rule be broadly inclusive of set-asides, reserves, partial set-asides, price evaluation preferences, source selection factors, and any other mechanisms which are not specifically addressed by the FAR. SBA does not feel that additional clarification is necessary and has adopted the proposed rule as final.

Deemed Certifications

One commenter expressed concern that proposed §§ 121.108(b)(2), 121.411(e)(2), 124.521(b)(2), 124.1015(b)(2), 125.29(b)(2), 126.900(b)(2), and 127.700(b)(2) are too broad and could permit attenuated acts or omissions to give rise to a deemed certification. SBA disagrees. Federal agencies are statutorily required to establish goals for the participation of small business concerns, SDVO small business concerns, HUBZone small business concerns, small disadvantaged business concerns, and WOSB concerns. 15 U.S.C. 644(g). At the conclusion of each fiscal year, Federal agencies must

compile reports as to the agencies' performance in attaining their contracting goals. 15 U.S.C. 644(h). It is SBA's intention that §§ 121.108(b)(2), 121.411(e)(2), 124.521(b)(2), 124.1015(b)(2), 125.29(b)(2), 126.900(b)(2), and 127.700(b)(2) shall be applied in cases where a specific offer encourages the procuring agency to classify the award as an award to a small business or other concern for the purposes of the agencies' contracting goals. Under 48 CFR § 4.1201, a Federal agency shall rely on a business concern's ORCA representations and certifications in determining how to classify the award. Accordingly, in most cases, it will be a firm's ORCA/SAM representations and certifications which would encourage a Federal agency to classify an award as having gone to a small business. Therefore, SBA believes that in practice, proposed §§ 121.108(b)(2), 121.411(e)(2), 124.521(b)(2), 124.1015(b)(2), 125.29(b)(2), 126.900(b)(2), and 127.700(b)(2) have a narrow application and the provisions have been adopted as final in this rule.

Another commenter recommended that SBA eliminate proposed §§ 121.108(b)(3), 121.411(e)(3), 124.521(b)(3), 124.1015(b)(3), 125.29(b)(3), 126.900(b)(3), and 127.700(b)(3), which provide that registration on any Federal electronic database for the purpose of being considered for award shall be deemed an affirmative, willful, and intentional certification as to the relevant concern's small business size and status. This is a statutory requirement that SBA cannot eliminate. The Jobs Act specifically deems registration on a Federal electronic database as a willful certification as to size and status. 15 U.S.C. § 632(w)(2)(C). As such, SBA is precluded by statute from eliminating these provisions and they remain in this final rule.

Signature Requirement

SBA received two comments regarding proposed §§ 121.108(c), 121.411(f), 124.521(c), 124.1015(c), 125.29(c), 126.900(c), 127.700(c), which require an authorized official to sign the small business size and status certification page of any solicitation, bid or proposal for a Federal grant, contract, subcontract, cooperative agreement, or cooperative research and development agreement reserved for small business concerns. The first commenter suggested that the rule specifically give electronic signatures the same effect as wet signatures. For the purpose of Government contracts, such a provision already exists at 48 CFR § 4.502(d) which provides that agencies may accept electronic signatures and records. However, SBA lacks the statutory authority to enact such a rule and has not adopted this comment.

The second commenter questioned whether the signature requirement is superfluous given that a signature on an offer is meant to certify all the offer's contents. SBA considered this comment, but has adopted the proposed provisions as final in this rule. The Jobs Act specifically requires that a certification as to a firm's small business size or other status shall contain the signature of an authorized official on the same page as the certification. 15 U.S.C. 632(w)(3)(B). As such, SBA is precluded by statute from eliminating the signature requirement. Further, the Federal Acquisition Council will implement the signature requirement in the Federal Acquisition Regulation and associated clauses. SBA has made minor wording changes in these provisions for clarity. The word "solicitation" has been replaced by the words "offer" and "proposal" to clarify that it is the offer that a contractor is signing, not the solicitation.

Limitation of Liability

Two commenters suggested that SBA amend proposed §§ 121.108(d), 121.411(g), 124.521(d), 124.1015(d), 125.29(d), 126.900(d), and 127.700(d) to adopt the statutory language which protects firms from liability where misrepresentation was the result of "unintentional errors, technical malfunctions, or other similar situations." SBA feels that the addition of "or other situations" more accurately captures the breadth of situations in which liability is to be limited and has therefore adopted this comment in the final rule.

Two commenters suggested that SBA clarify the standard of care required in making representations. Under proposed §§ 121.108(a), 121.411(d), 124.521(a), 124.1015(a), 125.29(a), 126.900(a), and 127.700(a), the presumption of loss applies only where a firm willfully misrepresents its small business size or other status. Sections 121.108(d), 121.411(g), 124.521(d), 124.1015(d), 125.29(d), 126.900(d), and 127.700(d) further provide that misrepresentations which are the result of "unintentional errors, technical malfunctions, or other similar situations" are not considered to be willful. In addition, the statute and implementing regulations provide that certain actions are deemed to be willful and require an official to sign on the same page as size or status representation. As discussed above, whether a representation is willful or should result in liability or criminal penalty is a fact-based decision that will be made by a judge, jury or other decider of fact. SBA has made minor wording changes in the limitation of liability provisions to make clear that the question of whether a misrepresentation is willful is a fact-based decision that will be made, not by SBA, but by a judge, jury or other decider of fact. To clarify that the limitation of liability provisions convey discretion to the finder of fact, the phrase "shall not apply" has been amended as "may be determined not to apply." Further, the phrase "consideration shall be given to" has been changed to "relevant factors to consider in making this determination may include."

One commenter asked if SBA would agree that thirty days is a reasonable amount of time in which to correct an erroneous representation. It is SBA's view that the question of whether an erroneous representation was corrected in a timely manner is dependent on the facts of a given case. SBA believes such a determination is best made by a judge, jury, or other decider of fact.

Two commenters suggested that business concerns be protected from liability when their misrepresentation resulted from ambiguity in SBA's regulations. As discussed above, SBA believes that a good faith misinterpretation of SBA's rules should not be considered a willful misrepresentation of size or status. Whether a regulation is ambiguous and whether a misinterpretation is reasonable and made in good faith is a fact- specific determination that will be made by a judge, jury, or other decider of fact.

Two commenters suggested that the list of mitigating factors set forth in the proposed rule be clarified and expanded. It is not SBA's intent that the list of mitigating factors included in the proposed rule be exhaustive. Again, the question of whether a firm willfully misrepresented its size or status is a factual determination best made by a judge, jury, or other decider of fact. SBA does not believe any additional changes or clarification is warranted.

Annual Recertification

One commenter argued that annual recertification is too burdensome. SBA disagrees. This rule does not impose new reporting requirements—concerns must certify their size and status annually in order to be identified as a small business or other socioeconomic concern in ORCA under existing regulations. 48 CFR § 4.1201(b).

Moreover, annual certification of size and status is statutorily required, 15 U.S.C. 632(x). In addition, a firm is expected to verify its representation in SAM every time it submits an offer on a government contract. SBA has, however, identified SAM as the current successor to ORCA and has amended all references to ORCA in the proposed rule to instead reference SAM. As such, SBA adopts the annual SAM verification requirement in this final rule.

Two commenters recommended that firms awarded contracts longer than five years be required to recertify only on the fifth year. SBA considered this comment but has adopted the proposed provisions as final. For purposes of establishing continuing eligibility for previously awarded long term contracts, recertification is required within 60 to 120 days prior to the end of the fifth year of the contract. 48 CFR § 52.219–28; 13 CFR § 121.404(g)(3). However, this requirement is distinct from the annual recertification requirements in the proposed rule. The annual recertification requirement contemplated in the proposed rule is for purposes of being considered for award of future contracts. Such a requirement already exists under 48 CFR § 4.1201(b). Accordingly, SBA has not adopted this comment in the Final rule.

One commenter suggested that SBA provide notification and an opportunity for business concerns to comply with the annual certification requirement. SBA does not believe such notification is necessary given that concerns are already required to certify their size and status annually under 48 CFR § 4.1201(b). Further, SBA lacks the statutory authority to implement such a notification system. Accordingly, SBA has not adopted this comment in the Final rule.

Another commenter suggested that SBA issue additional guidance to clarify the annual certification requirement as applied to business concerns operating in industries with a revenue-based size standard. This commenter expressed concern that an annual certification requirement would not take into consideration revenue fluctuations common to many small business concerns. SBA disagrees. At any given time, a firm's size may be determined under a revenue-based size standard by dividing the sum of firm's annual receipts from the past three completed fiscal years by three. 13 CFR § 121.104(c). This method is specifically designed to account for revenue fluctuations and SBA does not believe the annual recertification requirement has any implications specific to those firms operating in industries with revenue-based size standards.

Another commenter suggested that the annual recertification requirement be applied to 8(a) Business Development and HUBZone program participants. As noted in the proposed rule, SBA did not impose the recertification requirement for these programs because SBA is responsible for providing certification designations in federal procurement databases for these programs. Therefore, SBA has not adopted this comment in the final rule.

Other Comments

One commenter recommended that SBA provide clarification as to the rule's application to misrepresentations by subcontractors. It is SBA's intent that the presumption of loss shall apply to subcontractors who willfully misrepresent their size or status in order to receive a subcontract award. Accordingly, proposed §§ 121.108(a), 121.411(d), 124.521(a), 124.1015(a), 125.29(a), 126.900(a), and 127.700(a) explicitly provided that a presumption of loss to the United States shall be imposed whenever it is established that a business concern willfully sought and received award of a subcontract by misrepresentation. SBA does not believe any additional clarification is necessary. The same commenter also requested clarification of the prime contractor's liability when a subcontractor misrepresents its status to the prime contractor. Pursuant to 48 CFR § 19.703(b), a prime contractor acting in good faith may rely on the written representation of its subcontractor regarding the subcontractor's small business size or status. When read in conjunction with the final rule, SBA believes this insulates prime contractors acting in good faith from liability for misrepresentations made by their subcontractors. In response to this comment, SBA has clarified this point in the limitation of liability sections of the Final rule.

One commenter suggested that SBA provide clarification as to a contracting officer's duty to stop work on a contract if it becomes clear that the awardee misrepresented its status before completion of the contract. Under SBA's existing regulations, contracting officers have the authority to file a size protest at any time, even after award. 13 CFR §§ 121.1004(b), 124.1010(c)(1)(iii), 125.25(d)(3), 126.801(d)(3), and 127.603(c)(3). SBA's regulations also address the effect of a negative eligibility determination on the procurement in question. 13 CFR §§ 121.1009(g), 124.1013(h), 125.27(g), 126.803(d), and 127.604(f).

Another commenter suggested that SBA amend its regulations to impose suspension and debarment only when misrepresentation resulted in actual award. SBA does not believe that receipt of an award should be a prerequisite for debarment, suspension or any other penalty outlined in the Small Business Act or SBA's regulations. Firms have an obligation to accurately represent their size and/or status. Any fraudulent misrepresentation which inhibits the government's ability to rely on future statements made by the contractor should be subject to possible suspension and debarment actions. Accordingly this comment has not been adopted in the final rule. However, for clarity and accuracy, the title "debarring official" has been changed to "suspension and debarment official" in 13 CFR §§ 121.108(e)(1), 121.411(h)(1), 124.1015(e)(1), 125.29(e)(1), 126.900(e)(1), and 127.700(e)(1).

One commenter recommended that ORCA/SAM be modified to require the contractor to make an affirmative acknowledgment that the software interface correctly determined the business's size. Proposed §§ 121.108(c), 121.411(f), 124.521(c), 124.1015(c), 125.29(c), 126.900(c), 127.700(c) require an authorized official to sign the small business size and status certification page of any solicitation. SBA does not believe any additional clarification or changes to the proposed rule are necessary and adopts the provisions in the Final rule as proposed.

Another commenter suggested that SBA address situations where a firm claims to be small under its primary NAICS code and submits an offer on a procurement issued under a different NAICS code with a more restrictive size standard. SBA believes its regulations are clear on this point. 13 CFR § 121.402(a) provides that "a concern must not exceed the size standard for the NAICS code specified in the solicitation," and 13 CFR § 121.405(a) further provides that "a concern must self-certify it is small under the size standard specified in the solicitation." As such, SBA has not made additional changes to the rule in response to this comment.

One commenter recommended the creation of an IRS portal through which relevant parties may look up a business's tax returns for purposes of determining size. Tax returns are not public documents and SBA lacks the statutory authority to implement such a system.

One commenter proposed that footnote 18 to 13 CFR § 121.201 be applied to all value-added resellers. The proposed rule did not address specific

size standards and, therefore, this comment is beyond the scope of the proposed rulemaking.

Another commenter suggested that SBA eliminate all programs based on sex, race or minority status. The proposed rule did not address the elimination of any SBA programs and, therefore, this comment is beyond the scope of the proposed rulemaking.

Compliance with Executive Orders 12866, 13563, 12988, 13132, 13272, the Paperwork Reduction Act (44 U.S.C., Chapter 35) and the Regulatory Flexibility Act (5 U.S.C. 601–612)

Executive Order 12866

The Office of Management and Budget (OMB) has determined that this rule is a significant regulatory action for purposes of Executive Order 12866. In the proposed rule, SBA set forth its initial regulatory impact analysis, which addressed the following: Necessity of the regulation; the potential benefits and costs of the regulation; and alternative approaches to the proposed rule. SBA did not receive any comments which specifically addressed this regulatory impact analysis. Therefore, SBA adopts as final its initial regulatory impact analysis.

Executive Order 13563

This final rule implements important statutory provisions intended to prevent and deter fraud and misrepresentation in small business government contracting and other programs. SBA has amended all applicable Parts of its regulations to put participants in those programs on notice of the penalties associated with misrepresentation, and to the extent practicable, utilized identical language in each Part. SBA has also included in each Part other relevant applicable statutory provisions concerning the penalties for misrepresentation. The costs associated with these rules, requiring a signature in connection with a size or status representation and requiring concerns to update online certifications annually, are minimal and required by statute. As part of its implementation of this executive order and consistent with its commitment to public participation in the rulemaking process, SBA held public forums around the country to discuss implementation of the Jobs Act, including the provisions in this rule.

Executive Order 12988

For the purpose of Executive Order 12988, this final rule meets applicable standards set forth in section 3(a) and 3(b)(2) of Executive Order 12988, Civil Justice Reform, to minimize litigation, eliminate ambiguity, and reduce burden. This rule has no preemptive or retroactive effect.

Executive Order 13132

This final rule does not have federalism implications as defined in Executive Order 13132. It will not have substantial direct effects on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various layers of government, as specified in the order. As such it does not warrant the preparation of a Federalism Assessment.

Paperwork Reduction Act, 44 U.S.C., Ch. 35

For the purpose of the Paperwork Reduction Act, 44 U.S.C. Chapter 35, SBA has determined that this rule does not impose new reporting requirements and does not require new recordkeeping requirements. In accordance with 48 CFR §§ 4.1202, 52.204–6, 52.219–1 and 13 CFR §§ 121.404(a), 121.411, concerns must submit paper or electronic representations or certifications in connection with prime contracts and subcontracts. The Jobs Act requires that each offeror or applicant for a Federal contract, subcontract, or grant shall contain a certification concerning the small business size and status of a business concern seeking the Federal contract, subcontract or grant. The Jobs Act mandates that an authorized official must sign the certification on the same page containing the size and status claimed by the concern. Offerors are already required to sign their offers, bids or quotes (Standard Forms 18, 33, and 1449), so this provision does not create new reporting or recordkeeping requirements.

Regulatory Flexibility Act

SBA has determined that this rule may have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act (RFA), 5 U.S.C. 601–612. Accordingly, SBA set forth an Initial Regulatory Flexibility Act (IRFA) analysis in the proposed rule. The IRFA addressed the impact of the proposed rule in accordance with 5 U.S.C. 603. The IRFA examined the objectives and legal basis for the proposed rule; the kind and number of small entities that may be affected; the projected recordkeeping, reporting, and other requirements; whether there were any Federal rules that may duplicate, overlap, or conflict with the proposed rule; and whether there were any significant alternatives to the proposed rule. The Agency's final regulatory flexibility analysis (FRFA) is set forth below.

(a) Need for, Objectives, and Legal Basis of the Rule

These regulatory amendments implement Sections 1341 and 1342 of the Small Business Jobs Act of 2010, Public Law 111–240, 124 Stat. 2504, September 27, 2010 (Jobs Act); 15 U.S.C. 632(w), (x). The purpose of the statute and implementing regulations is to prevent or deter firms from misrepresenting their size or socioeconomic status.

(b) Estimate of the Number of Small Entities to Which the Rule Will Apply

The RFA directs agencies to provide a description of and, where feasible, an estimate of the number of entities that may be affected by the proposed rules, if adopted. The RFA defines "small entity" to include "small businesses," "small organizations," and "small governmental jurisdictions." SBA's programs do not apply to "small organizations" or "small governmental jurisdictions" because they are non-profit or governmental entities and do not generally qualify as "business concerns" within the meaning of SBA's regulations. SBA's programs generally apply only to for-profit business concerns. Therefore, the regulation will not impact small organizations or small governmental jurisdictions.

In fiscal year 2010, there were approximately 1.6 million small business contract actions (out of 3.36 million total small business eligible contract actions). This final rule's presumption of loss will only impact small business concerns that misrepresent their size or status in connection with a contract, subcontract, cooperative agreement, cooperative research and development agreement or grant in such a way that criminal prosecution or other action is taken by the Government in order to redress the misrepresentation. In fiscal year 2010, SBA found approximately 200 firms to be ineligible for a contract (14 HUBZone, 33 Service-Disabled Veteran-Owned, 0 Women-Owned Small Business, 151 size). Not all of these firms would be criminally prosecuted or have others actions taken against them. Thus, the regulations concerning presumption of loss will impact very few concerns, and some of these concerns are not actually small.

There are in approximately 348,000 concerns listed as small business concerns in the Dynamic Small Business Search (DSBS) database. The regulations concerning deemed certifications and the requirement for a

signature apply to all of these concerns, to the extent the concerns submit an offer for a prime contract that is set aside for small business concerns. In addition, there are small business concerns that are not registered in DSBS that submit offers or responses for grants, subcontracts, and other agreements. The annual certification requirement applies to all of the 348,000 firms registered in DSBS.

(c) Projected Reporting, Recordkeeping and Other Compliance Requirements

This final rule does not impose a new information collection, recordkeeping or compliance requirement on small businesses. A firm's size or socioeconomic status is generally based on records that it already possesses, such as payroll records and annual tax returns. Firms currently must represent their size or status in connection with contracts and subcontracts, either electronically or in paper form. 48 CFR §§ 4.1202, 52.204–8, 52.219–1 and 13 CFR §§ 121.404(a), 121.411. The rule requires an authorized official to sign on the page containing a concern's size or status representation. Offerors are already required to sign their offers, so the burden on small business concerns to also sign their size or status representation or certification is minimal. Standard Forms 18, 33, 1447 and 1449.

(d) Federal Rules Which May Duplicate, Overlap or Conflict With the Rule

Section 1342 of the Jobs Act requires that firms that fail to meet the annual certification or representation requirement shall lose their status in the database. Firms will not be able submit offers for small business contracts based on their online representations or certifications (48 CFR § 4.1201(c)), but instead must have an authorized official sign in connection with the firm's size or status. Firms must already sign offers, so the impact will be negligible. Standard Forms 18, 33, 1447 and 1449.

(e) Steps Taken To Minimize Impact on Small Entities

This final rule implements Sections 1341 and 1342 of the Jobs Act. The final rule is directed at small business concerns seeking government contracts, subcontracts, grants, and cooperative agreements. The final rule is intended to prevent or deter firms from misrepresenting their size or socioeconomic status. The impact on firms that accurately represent their size or status will be minimal. An authorized official will have to sign an offer where the firm represents its size and status, but authorized officials are currently required to sign offers. Firms will have to update their size and socioeconomic status in ORCA/SAM at least annually, but that too is already required. 48 CFR § 4.1201(b)(1).

(f) Issues Raised by Public Comments in Response to the Initial Regulatory Flexibility Analysis and the Agency's Assessment

The SBA received one comment that addressed the IRFA or the subjects discussed in the IRFA. This commenter expressed concern regarding a portion of the IRFA which read: "The proposed regulations concerning presumption of loss will only impact small business concerns that misrepresent their size or status in connection with a contract, subcontract, cooperative agreement, cooperative research and development agreement or grant in such a way that criminal prosecution or other action is taken by the Government." Specifically, the commenter felt that SBA's reference to "other action" requires clarification. As noted above, it is SBA's intent that the presumption of loss shall be applied in all manner of criminal, civil, administrative, contractual, common law, or other actions, which the United States government may take to redress willful misrepresentation. In fiscal year 2010, SBA found approximately 200 firms to be ineligible for a contract (14 HUBZone, 33 Service-Disabled Veteran-Owned, 0 Women-Owned Small Business, 151 size). Not all of these firms willfully misrepresented their size or status. Thus, SBA continues to believe that the regulations concerning presumption of loss will impact very few concerns, most of which will not qualify as small.

List of Subjects

13 CFR Part 121

Administrative practice and procedure, Reporting and recordkeeping requirements, and Small businesses.

13 CFR Part 124

Administrative practice and procedure, Minority businesses, Reporting and recordkeeping requirements, and Technical assistance.

13 CFR Part 125

Government contracts, Reporting and recordkeeping requirements, Small businesses, and Technical assistance.

13 CFR Part 126

Administrative practice and procedure, Penalties, Reporting and recordkeeping requirements and Small businesses.

13 CFR Part 127

Government procurement, Reporting and recordkeeping requirements, and Small businesses.

For the reasons stated in the preamble, SBA amends parts 121, 124, 125, 126 and 127 of title 13 of the Code of Federal Regulations as follows:

PART 121—SMALL BUSINESS SIZE REGULATIONS

■ 1. The authority citation for part 121 continues to read as follows:

Authority: 15 U.S.C. 632, 634(b)(6), 636(b), 637(a), 644 and 662(5); and Pub. L. 105–135, sec. 401 et seq., 111 Stat. 2592.

■ 2. Revise § 121.108 to read as follows:

§ 121.108 What are the requirements for representing small business size status, and what are the penalties for misrepresentation?

(a) *Presumption of Loss Based on the Total Amount Expended.* In every contract, subcontract, cooperative agreement, cooperative research and development agreement, or grant which is set aside, reserved, or otherwise classified as intended for award to small business concerns, there shall be a presumption of loss to the United States based on the total amount expended on the contract, subcontract, cooperative agreement, cooperative research and development agreement, or grant whenever it is established that a business concern other than a small business concern willfully sought and received the award by misrepresentation.

(b) *Deemed Certifications.* The following actions shall be deemed affirmative, willful and intentional certifications of small business size and status:

(1) Submission of a bid, proposal, application or offer for a Federal grant, contract, subcontract, cooperative agreement, or cooperative research and development agreement reserved, set aside, or otherwise classified as intended for award to small business concerns.

(2) Submission of a bid, proposal, application or offer for a Federal grant, contract, subcontract, cooperative agreement or cooperative research and development agreement which in any way encourages a Federal agency to classify the bid or proposal, if awarded, as an award to a small business concern.

(3) Registration on any Federal electronic database for the purpose of being considered for award of a Federal grant, contract, subcontract, cooperative agreement, or cooperative research and

development agreement, as a small business concern.

(c) *Signature Requirement.* Each offer, proposal, bid, or application for a Federal contract, subcontract, or grant shall contain a certification concerning the small business size and status of a business concern seeking the Federal contract, subcontract or grant. An authorized official must sign the certification on the same page containing the size status claimed by the concern.

(d) *Limitation of Liability.* Paragraphs (a) through (c) of this section may be determined not to apply in the case of unintentional errors, technical malfunctions, and other similar situations that demonstrate that a misrepresentation of size was not affirmative, intentional, willful or actionable under the False Claims Act, 31 U.S.C. §§ 3729, et seq. A prime contractor acting in good faith should not be held liable for misrepresentations made by its subcontractors regarding the subcontractors' size. Relevant factors to consider in making this determination may include the firm's internal management procedures governing size representation or certification, the clarity or ambiguity of the representation or certification requirement, and the efforts made to correct an incorrect or invalid representation or certification in a timely manner. An individual or firm may not be held liable where government personnel have erroneously identified a concern as small without any representation or certification having been made by the concern and where such identification is made without the knowledge of the individual or firm.

(e) *Penalties for Misrepresentation.*

(1) *Suspension or debarment.* The SBA suspension and debarment official or the agency suspension and debarment official may suspend or debar a person or concern for misrepresenting a firm's size status pursuant to the procedures set forth in 48 CFR subpart 9.4.

(2) *Civil Penalties.* Persons or concerns are subject to severe penalties under the False Claims Act, 31 U.S.C. 3729–3733, and under the Program Fraud Civil Remedies Act, 331 U.S.C. 3801–3812, and any other applicable laws.

(3) *Criminal Penalties.* Persons or concerns are subject to severe criminal penalties for knowingly misrepresenting the small business size status of a concern in connection with procurement programs pursuant to section 16(d) of the Small Business Act, 15 U.S.C. 645(d), as amended, 18 U.S.C. 1001, 18 U.S.C. 287, and any other applicable laws. Persons or concerns are subject to criminal penalties for knowingly making false statements or misrepresentations to SBA for the purpose of influencing any actions of SBA pursuant to section 16(a) of the Small Business Act, 15 U.S.C. 645(a), as amended, including failure to correct "continuing representations" that are no longer true.

■ 3. Add new § 121.109 to read as follows:

§ 121.109 What must a concern do in order to be identified as a small business concern in any Federal procurement databases?

(a) In order to be identified as a small business concern in the System for Award Management (SAM) database (or any successor thereto), a concern must certify its size in connection with specific size standards at least annually.

(b) If a firm identified as a small business concern in SAM fails to certify its size within one year of a size certification, the firm will not be listed as a small business concern in SAM, unless and until the firm recertifies its size.

§ 121.404 [Amended]

■ 4. Amend § 121.404(b) by removing "and the date of certification by SBA" and adding in its place "and, where applicable, the date the SBA program office requests a formal size determination in connection with a concern that otherwise appears eligible for program certification."

■ 5. Amend § 121.411 by adding new paragraphs (d) through (i) to read as follows:

§ 121.411 What are the size procedures for SBA's section 8(d) Subcontracting Program?

* * * * *

(d) *Presumption of Loss Based on the Total Amount Expended.* In every contract, subcontract, cooperative agreement, cooperative research and development agreement, or grant which is set aside, reserved, or otherwise classified as intended for award to small business concerns, there shall be a presumption of loss to the United States based on the total amount expended on the contract, subcontract, cooperative agreement, cooperative research and development agreement, or grant whenever it is established that a business concern other than a small business concern willfully sought and received the award by misrepresentation.

(e) *Deemed Certifications.* The following actions shall be deemed affirmative, willful and intentional certifications of small business size and status:

(1) Submission of a bid, proposal, application or offer for a Federal grant, contract, subcontract, cooperative agreement, or cooperative research and development agreement reserved, set aside, or otherwise classified as intended for award to small business concerns.

(2) Submission of a bid, proposal, application or offer for a Federal grant, contract, subcontract, cooperative agreement or cooperative research and development agreement which in any way encourages a Federal agency to classify the bid or proposal, if awarded, as an award to a small business concern.

(3) Registration on any Federal electronic database for the purpose of being considered for award of a Federal grant, contract, subcontract, cooperative agreement, or cooperative research and development agreement, as a small business concern.

(f) *Signature Requirement.* Each offer, proposal, bid, or application for a Federal contract, subcontract, or grant shall contain a certification concerning the small business size and status of a business concern seeking the Federal contract, subcontract or grant. An authorized official must sign the certification on the same page containing the size status claimed by the concern.

(g) *Limitation of Liability.* Paragraphs (d) through (f) of this section may be determined not to apply in the case of unintentional errors, technical malfunctions, and other similar situations that demonstrate that a misrepresentation of size was not affirmative, intentional, willful or actionable under the False Claims Act, 31 U.S.C. §§ 3729, et seq. A prime contractor acting in good faith should not be held liable for misrepresentations made by its subcontractors regarding the subcontractors' size. Relevant factors to consider in making this determination may include the firm's internal management procedures governing size representation or certification, the clarity or ambiguity of the representation or certification requirement, and the efforts made to correct an incorrect or invalid representation or certification in a timely manner. An individual or firm may not be held liable where government personnel have erroneously identified a concern as small without any representation or certification having been made by the concern and where such identification is made without the knowledge of the individual or firm.

(h) *Penalties for Misrepresentation.*

(1) *Suspension or debarment.* The SBA suspension and debarment official or the agency suspension and debarment official may suspend or debar a person or concern for misrepresenting a firm's size status pursuant to the procedures set forth in 48 CFR subpart 9.4.

(2) *Civil Penalties.* Persons or concerns are subject to severe penalties under the False Claims Act, 31 U.S.C. 3729–3733, and under the Program Fraud Civil Remedies Act, 331 U.S.C. 3801–3812, and any other applicable laws.

(3) *Criminal Penalties.* Persons or concerns are subject to severe criminal penalties for knowingly misrepresenting the small business size status of a concern in connection with procurement programs pursuant to section 16(d) of the Small Business Act, 15 U.S.C. 645(d), as amended, 18 U.S.C. 1001, 18 U.S.C. 287, and any other applicable laws. Persons or concerns are subject to criminal penalties for knowingly making false statements or misrepresentations to SBA for the purpose of influencing any actions of SBA pursuant to section 16(a) of the Small Business Act, 15 U.S.C. 645(a), as amended, including failure to correct "continuing representations" that are no longer true.

■ 6. Revise paragraph (f) of § 121.1009 to read as follows:

§ 121.1009 What are the procedures for making size determinations?

* * * * *

(f) *Notification of determination.* SBA will promptly notify the contracting officer, the protester, and the protested concern. SBA will send the notification by verifiable means, which may include facsimile, electronic mail, or overnight delivery service.

* * * * *

PART 124—8(a) BUSINESS DEVELOPMENT/SMALL DISADVANTAGED BUSINESS STATUS DETERMINATIONS

■ 7. The authority citation for part 124 continues to read as follows:

Authority: 15 U.S.C. 634(b)(6), 636(j), 637(a), 637(d) and Pub. L. 99–661, Pub. L. 100–656, sec. 1207, Pub. L. 101–37, Pub. L. 103–574, section 8021, Pub. L. 108–87, and 42 U.S.C. 9815.

■ 8. Add new § 124.521 to read as follows:

§ 124.521 What are the requirements for representing 8(a) status, and what are the penalties for misrepresentation?

(a) *Presumption of Loss Based on the Total Amount Expended.* In every contract, subcontract, cooperative agreement, cooperative research and development agreement, or grant which is set aside, reserved, or otherwise classified as intended for award to 8(a) Participants, there shall be a presumption of loss to the United States based on the total amount expended on the contract, subcontract, cooperative agreement, cooperative research and development agreement, or grant whenever it is established that a business concern other than an 8(a) Participant willfully sought and received the award by misrepresentation.

(b) *Deemed Certifications.* The following actions shall be deemed affirmative, willful and intentional certifications of 8(a) status:

(1) Submission of a bid or proposal for an 8(a) sole source or competitive contract.

(2) Registration on any Federal electronic database for the purpose of being considered for award of a Federal grant, contract, subcontract, cooperative agreement, or cooperative research and development agreement, as a small disadvantaged business (SDB).

(c) *Signature Requirement.* Each offer for an 8(a) contract shall contain a certification concerning the 8(a) status of a business concern seeking the contract. An authorized official must sign the certification on the same page containing the 8(a) status claimed by the concern.

(d) *Limitation of Liability.* Paragraphs (a)–(c) of this section may be determined not to apply in the case of unintentional errors, technical malfunctions, and other similar situations that demonstrate that a misrepresentation of 8(a) status was not affirmative, intentional, willful or actionable under the False Claims Act, 31 U.S.C. 3729, et seq. A prime contractor acting in good faith should not be held liable for misrepresentations made by its subcontractors regarding the subcontractors' 8(a) status. Relevant factors to consider in making this determination may include the firm's internal management procedures governing representation or certification as an eligible 8(a) Participant, the clarity or ambiguity of the representation or certification requirement, and the efforts made to correct an incorrect or invalid representation or certification in a timely manner. An individual or firm may not be held liable where government personnel have erroneously identified a concern as an eligible 8(a) Participant without any representation or certification having been made by the concern and where such identification is made without the knowledge of the individual or firm.

■ 9. Add new § 124.1015 to read as follows:

§ 124.1015 What are the requirements for representing SDB status, and what are the penalties for misrepresentation?

(a) *Presumption of Loss Based on the Total Amount Expended.* In every contract, subcontract, cooperative agreement, cooperative research and development agreement, or grant which is set aside, reserved, or otherwise classified as intended for award to SDB concerns, there shall be a presumption of loss to the United States based on the total amount expended on the contract, subcontract, cooperative agreement, cooperative research and development agreement, or grant whenever it is established that a business concern other than a SDB willfully sought and received the award by misrepresentation.

(b) *Deemed Certifications.* The following actions shall be deemed affirmative, willful and intentional certifications of SDB status:

(1) Submission of a bid, proposal, application or offer for a Federal grant, contract, subcontract, cooperative agreement, or cooperative research and development agreement reserved, set aside, or otherwise classified as intended for award to SDBs.

(2) Submission of a bid, proposal, application or offer for a Federal grant, contract, subcontract, cooperative agreement or cooperative research and development agreement which in any way encourages a Federal agency to classify the bid or proposal, if awarded, as an award to a SDB.

(3) Registration on any Federal electronic database for the purpose of being considered for award of a Federal grant, contract, subcontract, cooperative agreement, or cooperative research and development agreement, as a SDB.

(c) *Signature Requirement.* Each offer, proposal, bid, or application for a Federal contract, subcontract, or grant shall contain a certification concerning the SDB status of a business concern seeking the Federal contract, subcontract or grant. An authorized official must sign the certification on the same page containing the SDB status claimed by the concern.

(d) *Limitation of Liability.* Paragraphs (a) through (c) of this section may be determined not to apply in the case of unintentional errors, technical malfunctions, and other similar

situations that demonstrate that a misrepresentation of SDB status was not affirmative, intentional, willful or actionable under the False Claims Act, 31 U.S.C. 3729, et seq. A prime contractor acting in good faith should not be held liable for misrepresentations made by its subcontractors regarding the subcontractors' SDB status. Relevant factors to consider in making this determination may include the firm's internal management procedures governing SDB status representation or certification, the clarity or ambiguity of the representation or certification requirement, and the efforts made to correct an incorrect or invalid representation or certification in a timely manner. An individual or firm may not be held liable where government personnel have erroneously identified a concern as a SDB without any representation or certification having been made by the concern and where such identification is made without the knowledge of the individual or firm.

(e) *Penalties for Misrepresentation.*

(1) *Suspension or debarment.* The SBA suspension and debarment official or the agency suspension and debarment official may suspend or debar a person or concern for misrepresenting a firm's status as a SDB pursuant to the procedures set forth in 48 CFR subpart 9.4.

(2) *Civil Penalties.* Persons or concerns are subject to severe penalties under the False Claims Act, 31 U.S.C. 3729–3733, and under the Program Fraud Civil Remedies Act, 331 U.S.C. 3801–3812, and any other applicable laws.

(3) *Criminal Penalties.* Persons or concerns are subject to severe criminal penalties for knowingly misrepresenting the SDB status of a concern in connection with procurement programs pursuant to section 16(d) of the Small Business Act, 15 U.S.C. 645(d), as amended, 18 U.S.C. 1001, 18 U.S.C. 287, and any other applicable laws. Persons or concerns are subject to criminal penalties for knowingly making false statements or misrepresentations to SBA for the purpose of influencing any actions of SBA pursuant to section 16(a) of the Small Business Act, 15 U.S.C. 645(a), as amended, including failure to correct "continuing representations" that are no longer true.

■ 10. Add new § 124.1016 to read as follows:

§ 124.1016 What must a concern do in order to be identified as a SDB in any Federal procurement database?

(a) In order to be identified as a SDB in the System for Award Management (SAM) database (or any successor thereto), a concern must certify its SDB status in connection with specific eligibility requirements at least annually.

(b) If a firm identified as a SDB in SAM fails to certify its status within one year of a status certification, the firm will not be listed as a SDB in SAM, unless and until the firm recertifies its SDB status.

PART 125—GOVERNMENT CONTRACTING PROGRAMS

■ 11. The authority citation for part 125 is revised to read as follows:

Authority: 15 U.S.C. 632, 634(b)(6), 637, 644 and 657f.

■ 12. Revise § 125.29 to read as follows:

§ 125.29 What are the requirements for representing SDVO SBC status, and what are the penalties for misrepresentation?

(a) *Presumption of Loss Based on the Total Amount Expended.* In every contract, subcontract, cooperative agreement, cooperative research and development agreement, or grant which is set aside, reserved, or otherwise classified as intended for award to SDVO SBCs, there shall be a presumption of loss to the United States based on the total amount expended on the contract, subcontract, cooperative agreement, cooperative research and development agreement, or grant whenever it is established that a business concern other than a SDVO SBC willfully sought and received the award by misrepresentation.

(b) *Deemed Certifications.* The following actions shall be deemed affirmative, willful and intentional certifications of SDVO SBC status:

(1) Submission of a bid, proposal, application or offer for a Federal grant, contract, subcontract, cooperative agreement, or cooperative research and development agreement reserved, set aside, or otherwise classified as intended for award to SDVO SBCs.

(2) Submission of a bid, proposal, application or offer for a Federal grant, contract, subcontract, cooperative agreement or cooperative research and development agreement which in any way encourages a Federal agency to classify the bid or proposal, if awarded, as an award to a SDVO SBC.

(3) Registration on any Federal electronic database for the purpose of being considered for award of a Federal grant, contract, subcontract, cooperative agreement, or cooperative research and development agreement, as a SDVO SBC.

(c) *Signature Requirement.* Each offer, proposal, bid, or application for a Federal contract, subcontract, or grant shall contain a certification concerning the SDVO SBC status of a business concern seeking the Federal contract, subcontract or grant. An authorized official must sign the certification on the same page containing the SDVO SBC status claimed by the concern.

(d) *Limitation of Liability.* Paragraphs (a) through (c) of this section may be determined not to apply in the case of unintentional errors, technical malfunctions, and other similar situations that demonstrate that a misrepresentation of SDVO SBC status was not affirmative, intentional, willful or actionable under the False Claims Act, 31 U.S.C. §§ 3729, et seq. A prime contractor acting in good faith should not be held liable for misrepresentations made by its subcontractors regarding the subcontractors' SDVO SBC status. Relevant factors to consider in making this determination may include the firm's internal management procedures governing SDVO SBC status representations or certifications, the clarity or ambiguity of the representation or certification requirement, and the efforts made to correct an incorrect or invalid representation or certification in a timely manner. An individual or firm may not be held liable where government personnel have erroneously identified a concern as a SDVO SBC without any representation or certification having been made by the concern and where such identification is made without the knowledge of the individual or firm.

(e) *Penalties for Misrepresentation.*

(1) *Suspension or debarment.* The SBA suspension and debarment official or the agency suspension and debarment official may suspend or debar a person or concern for misrepresenting a firm's status as a SDVO SBC pursuant to the procedures set forth in 48 CFR subpart 9.4.

(2) *Civil Penalties.* Persons or concerns are subject to severe penalties under the False Claims Act, 31 U.S.C. 3729–3733, and under the Program Fraud Civil Remedies Act, 331 U.S.C. 3801–3812, and any other applicable laws.

(3) *Criminal Penalties.* Persons or concerns are subject to severe criminal penalties for knowingly misrepresenting the SDVO SBC status of a concern in connection with procurement programs pursuant to section 16(d) of the Small Business Act, 15 U.S.C. 645(d), as amended, 18 U.S.C. 1001, 18 U.S.C. 287, and any other applicable laws. Persons or concerns are subject to criminal penalties for knowingly making false statements or misrepresentations to SBA

for the purpose of influencing any actions of SBA pursuant to section 16(a) of the Small Business Act, 15 U.S.C. 645(a), as amended, including failure to correct "continuing representations" that are no longer true.

■ 13. Add new § 125.30 to read as follows:

§ 125.30 What must a concern do in order to be identified as a SDVO SBC in any Federal procurement databases?

(a) In order to be identified as a SDVO SBC in the System for Award Management (SAM) database (or any successor thereto), a concern must certify its SDVO SBC status in connection with specific eligibility requirements at least annually.

(b) If a firm identified as a SDVO SBC in SAM fails to certify its status within one year of a status certification, the firm will not be listed as a SDVO SBC in SAM, unless and until the firm recertifies its SDVO SBC status.

PART 126—HUBZONE PROGRAM

■ 14. The authority citation for part 126 continues to read as follows:

Authority: 15 U.S.C. 632(a), 632(j), 632(p) and 657a.

■ 15. Revise § 126.900 to read as follows:

§ 126.900 What are the requirements for representing HUBZone status, and what are the penalties for misrepresentation?

(a) *Presumption of Loss Based on the Total Amount Expended.* In every contract, subcontract, cooperative agreement, cooperative research and development agreement, or grant which is set aside, reserved, or otherwise classified as intended for award to HUBZone SBCs, there shall be a presumption of loss to the United States based on the total amount expended on the contract, subcontract, cooperative agreement, cooperative research and development agreement, or grant whenever it is established that a business concern other than a HUBZone SBC willfully sought and received the award by misrepresentation.

(b) *Deemed Certifications.* The following actions shall be deemed affirmative, willful and intentional certifications of HUBZone SBC status:

(1) Submission of a bid, proposal, application or offer for a Federal grant, contract, subcontract, cooperative agreement, or cooperative research and development agreement reserved, set aside, or otherwise classified as intended for award to HUBZone SBCs.

(2) Submission of a bid, proposal, application or offer for a Federal grant, contract, subcontract, cooperative agreement or cooperative research and development agreement which in any way encourages a Federal agency to classify the bid or proposal, if awarded, as an award to a HUBZone SBC.

(3) Registration on any Federal electronic database for the purpose of being considered for award of a Federal grant, contract, subcontract, cooperative agreement, or cooperative research and development agreement, as a HUBZone SBC.

(c) *Signature Requirement.* Each offer, proposal, bid, or application for a Federal contract, subcontract, or grant shall contain a certification concerning the HUBZone SBC status of a business concern seeking the Federal contract, subcontract or grant. An authorized official must sign the certification on the same page containing the HUBZone status claimed by the concern.

(d) *Limitation of Liability.* Paragraphs (a)–(c) of this section may be determined not to apply in the case of unintentional errors, technical malfunctions, and other similar situations that demonstrate that a misrepresentation of HUBZone status was not affirmative, intentional, willful or actionable under the False Claims Act, 31 U.S.C. §§ 3729, et seq. A prime contractor acting in good faith should not be held liable for misrepresentations made by its subcontractors regarding the subcontractors' HUBZone status. Relevant factors to consider in making this determination may include the firm's internal management procedures governing HUBZone status representations or certifications, the clarity or ambiguity of the representation or certification requirement, and the efforts made to correct an incorrect or invalid representation or certification in a timely manner. An individual or firm may not be held liable where government personnel have erroneously identified a concern as a HUBZone SBC without any representation or certification having been made by the concern and where such identification is made without the knowledge of the individual or firm.

(e) *Penalties for Misrepresentation.*

(1) *Suspension or debarment.* The SBA suspension and debarment official or the agency suspension and debarment official may suspend or debar a person or concern for misrepresenting a firm's status as a HUBZone SBC pursuant to the procedures set forth in 48 CFR subpart 9.4.

(2) *Civil Penalties.* Persons or concerns are subject to severe penalties under the False Claims Act, 31 U.S.C. 3729–3733, and under the Program Fraud Civil Remedies Act, 331 U.S.C. 3801–3812, and any other applicable laws.

(3) *Criminal Penalties.* Persons or concerns are subject to severe criminal penalties for knowingly misrepresenting the HUBZone status of a concern in connection with procurement programs pursuant to section 16(d) of the Small Business Act, 15 U.S.C. 645(d), as amended, 18 U.S.C. 1001, 18 U.S.C. 287, and any other applicable laws. Persons or concerns are subject to criminal penalties for knowingly making false statements or misrepresentations to SBA for the purpose of influencing any actions of SBA pursuant to section 16(a) of the Small Business Act, 15 U.S.C. 645(a), as amended, including failure to correct "continuing representations" that are no longer true.

PART 127—WOMEN-OWNED SMALL BUSINESS FEDERAL CONTRACT PROGRAM

■ 16. The authority citation for part 127 is revised to read as follows:

Authority: 15 U.S.C. 632, 634(b)(6), 637(m), and 644.

■ 17. Revise § 127.700 to read as follows:

§ 127.700 What are the requirements for representing EDWOSB or WOSB status, and what are the penalties for misrepresentation?

(a) *Presumption of Loss Based on the Total Amount Expended.* In every contract, subcontract, cooperative agreement, cooperative research and development agreement, or grant which is set aside, reserved, or otherwise classified as intended for award to EDWOSBs or WOSBs, there shall be a presumption of loss to the United States based on the total amount expended on the contract, subcontract, cooperative agreement, cooperative research and development agreement, or grant whenever it is established that a business concern other than a EDWOSB or WOSB willfully sought and received the award by misrepresentation.

(b) *Deemed Certifications.* The following actions shall be deemed affirmative, willful and intentional certifications of EDWOSB or WOSB status:

(1) Submission of a bid, proposal, application or offer for a Federal grant, contract, subcontract, cooperative agreement, or cooperative research and development agreement reserved, set aside, or otherwise classified as intended for award to EDWOSBs or WOSBs.

(2) Submission of a bid, proposal, application or offer for a Federal grant, contract, subcontract, cooperative agreement or cooperative research and development agreement which in any way encourages a Federal agency to classify the bid or proposal, if awarded, as an award to a EDWOSB or WOSB.

(3) Registration on any Federal electronic database for the purpose of being considered for award of a Federal grant, contract, subcontract, cooperative agreement, or cooperative research and development agreement, as an EDWOSB or WOSB.

(c) *Signature Requirement.* Each offer, proposal, bid, or application for a Federal contract, subcontract, or grant shall contain a certification concerning the EDWOSB or WOSB status of a business concern seeking the Federal contract, subcontract or grant. An authorized official must sign the certification on the same page containing the EDWOSB or WOSB status claimed by the concern.

(d) *Limitation of Liability.* Paragraphs (a)–(c) of this section may be determined not to apply in the case of unintentional errors, technical malfunctions, and other similar situations that demonstrate that a misrepresentation of EDWOSB or WOSB status was not affirmative, intentional, willful or actionable under the False Claims Act, 31 U.S.C. §§ 3729, et seq. A prime contractor acting in good faith should not be held liable for misrepresentations made by its subcontractors regarding the subcontractors' EDWOSB or WOSB status. Relevant factors to consider in making this determination may include the firm's internal management procedures governing EDWOSB or WOSB status representations or certifications, the clarity or ambiguity of the representation or certification requirement, and the efforts made to correct an incorrect or invalid representation or certification in a timely manner. An individual or firm may not be held liable where government personnel have erroneously identified a concern as an EDWOSB or WOSB without any representation or certification having been made by the concern and where such identification is made without the knowledge of the individual or firm.

(e) *Penalties for Misrepresentation.*

(1) *Suspension or debarment.* The SBA suspension and debarment official or the agency suspension and debarment official may suspend or debar a person or concern for misrepresenting a firm's status as an EDWOSB or WOSB pursuant to the procedures set forth in 48 CFR subpart 9.4.

(2) *Civil Penalties.* Persons or concerns are subject to severe penalties under the False Claims Act, 31 U.S.C. 3729–3733, and under the Program Fraud Civil Remedies Act, 331 U.S.C. 3801–3812, and any other applicable laws.

(3) *Criminal Penalties.* Persons or concerns are subject to severe criminal penalties for knowingly misrepresenting the EDWOSB or WOSB status of a concern in connection with procurement programs pursuant to section 16(d) of the Small Business Act, 15 U.S.C. 645(d), as amended, 18 U.S.C. 1001, 18 U.S.C. 287, and any other applicable laws. Persons or concerns are subject to criminal penalties for knowingly making false statements or misrepresentations to SBA for the purpose of influencing any actions of SBA pursuant to section 16(a) of the Small Business Act, 15 U.S.C. 645(a), as amended, including failure to correct "continuing representations" that are no longer true.

■ 18. Add new § 127.701 to read as follows:

§ 127.701 What must a concern do in order to be identified as an EDWOSB or WOSB in any Federal procurement databases?

(a) In order to be identified as an EDWOSB or WOSB in the System for Award Management (SAM) database (or any successor thereto), a concern must certify its EDWOSB or WOSB status in connection with specific eligibility requirements at least annually.

(b) If a firm identified as an EDWOSB or WOSB in SAM fails to certify its status within one year of a status certification, the firm will not be listed as an EDWOSB or WOSB in SAM, unless and until the firm recertifies its EDWOSB or WOSB status.

Karen G. Mills,

Administrator.

[FR Doc. 2013–15418 Filed 6–27–13; 8:45 am]

BILLING CODE 8025–01–P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 39

[Docket No. FAA–2012–1214; Directorate Identifier 2011–SW–071–AD; Amendment 39–17482; AD 2013–12–04]

RIN 2120–AA64

Airworthiness Directives; Eurocopter France Helicopters

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final rule.

SUMMARY: We are adopting a new airworthiness directive (AD) for Eurocopter France Model EC 155B, EC155B1, SA–366G1, SA–365N, SA–365N1, AS–365N2, and AS 365 N3 helicopters, which requires modifying the fuel tank draining system. This AD is prompted by a closed fuel tank drain that, in the event of a fuel leak, could result in fuel accumulating in an area containing electrical equipment. The actions are intended to prevent accumulation of fuel in an area with electrical equipment or another ignition source, which may lead to a fire.

DATES: This AD is effective August 2, 2013.

The Director of the Federal Register approved the incorporation by reference of certain documents listed in this AD as of August 2, 2013.

ADDRESSES: For service information identified in this AD, contact American Eurocopter Corporation, 2701 N. Forum Drive, Grand Prairie, TX 75052; telephone (972) 641–0000 or (800) 232–0323; fax (972) 641–3775; or at *http://www.eurocopter.com/techpub.* You may review the referenced service information at the FAA, Office of the Regional Counsel, Southwest Region, 2601 Meacham Blvd., Room 663, Fort Worth, Texas 76137.

Examining the AD Docket

You may examine the AD docket on the Internet at *http://www.regulations.gov* or in person at the Docket Operations Office between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The AD docket contains this AD, any incorporated-by-reference service information, the economic evaluation, any comments received, and other information. The street address for the Docket Operations Office (phone: 800–647–5527) is U.S. Department of Transportation, Docket Operations Office, M–30, West Building Ground Floor, Room W12–140, 1200 New Jersey Avenue SE., Washington, DC 20590.

Exhibit 3:

Microtechnologies, LLC Notice of Proposed Debarment Letter

U.S. SMALL BUSINESS ADMINISTRATION
WASHINGTON, DC 20416

December 20, 2013

VIA CERTIFIED MAIL – RETURN RECEIPT

Microtechnologies, LLC
8330 Boone Blvd.
Suite 600
Vienna, VA 22182-2624

Anthony Jimenez
1107 Robindale Drive
Great Falls, VA 22066-1800

Re: Notice of Proposed Debarment

Dear Mr. Jimenez:

I am the Suspension and Debarment Official at the U.S. Small Business Administration (SBA). SBA is proposing to debar Microtechnologies, LLC d/b/a MicroTech (MicroTech) (Duns: 145454182, and 078468018), and Mr. Anthony Jimenez from future contracting with any agency of the Executive Branch of the United States Government under Section 9.406 of the Federal Acquisition Regulation (FAR), Title 48 of the Code of Federal Regulations (CFR). This letter notifies you of your opportunity to submit a response for my consideration as the SBA's Suspension and Debarment Official.

I am proposing the debarment of MicroTech, and Mr. Jimenez based on information showing that Mr. Jimenez and MicroTech submitted false and misleading statements to the SBA in connection with MicroTech's application to participate in SBA's 8(a) Business Development (BD) Program. As the President/CEO and Managing Member of MicroTech, Mr. Jimenez is responsible for and is assumed to be aware of information submitted to SBA on behalf of MicroTech, and therefore the conduct of MicroTech in submitting false and/or misleading information to SBA may be properly imputed to Mr. Jimenez. Mr. Jimenez is being proposed for debarment based on his own conduct and as an affiliate[1] of MicroTech.

[1] Affiliates." Business concerns, organizations, or individuals are affiliates of each other if, directly or indirectly, (1) either one controls or has the power to control the other, or (2) a third party controls or has the power to control both. Indicia of control include, but are not limited to, interlocking management or ownership, identity of interests among family members, shared facilities and equipment, common use of employees, or a business entity organized following the debarment, suspension, or proposed debarment of a contractor which has the same or similar management, ownership, or principal employees as the contractor that was debarred, suspended, or proposed for debarment. FAR 9.403

SBA's 8(a) BD program provides companies meeting the qualifications for program participation additional opportunities to obtain Government contracts. The program provides these opportunities in order to assist in the overall business development of 8(a) participant firms. 8(a) BD participants are eligible for both set-aside and sole source contracts (collectively 8(a) BD contracts). 13 C.F.R. § 124.501(b).

8(a) BD participants, with exceptions not relevant to this matter, must be managed on a full-time basis by one or more disadvantaged individuals. 13 C.F.R. § 124.106(a)(1). SBA may deny admission to the 8(a) BD program if SBA learns that an applicant submitted false information during the application process, notwithstanding whether that information was material. 13 C.F.R. § 124.108(a)(5).

SBA may debar a person or business for any reason listed in FAR § 9.406-2, when there is a preponderance of evidence to suspect a person (including a corporation) has committed an offense in connection with the performance of a public contract. According to the FAR:

> The debarring official may debar –
> (a) A contractor for a conviction of or civil judgment for –
> (1) Commission of fraud or a criminal offense in connection with
> (i) Obtaining;
> (ii) Attempting to obtain; or
> (iii) Performing a public contract or subcontract; . . .
> (c) A contractor or subcontractor based on any other cause of so serious or compelling a nature that it affects the present responsibility of a Government contractor or subcontractor.

FAR § 9.406-2(a)(1) and (c).

SBA believes that MicroTech's present responsibility is questionable due to the false and misleading information contained in its 8(a) BD application. Mr. Jimenez submitted an application for SBA's 8(a) BD program on behalf of MicroTech in April 2005. On April 15, 2005 and May 4, 2005 SBA asked for additional documents and information from MicroTech and Mr. Jimenez regarding the relationships between MicroTech, its owners and officers, and two other firms, MicroLink, LLC (MicroLink), and GovWare, LLC (GovWare). The information shows that MicroTech's two minority equity holders, Mr. Timothy Wharton (Mr. Wharton), and Mr. David Truitt (Mr. Truitt) were the sole owners of MicroLink, as well as partial owners of GovWare.

SBA's request for information about GovWare, stated the following, "Explain the relationship if any, between Govware, LLC and Microtech, LLC." SBA also requested that Mr. Jimenez provide corporate documents for GovWare, as well as tax returns for the firm. In response to this request Mr. Jimenez and MicroTech provided GovWare's Operating Agreement, including recent changes and amendments, and the firm's recent tax returns. Mr. Jimenez and MicroTech also provided this statement:

> Until January 1, 2005, Anthony Jimenez had controlling ownership in Govware,

> LLC. In an effort to devote the entirety of his time to the management and running of MicroTech, LLC on January 1, 2005 Mr. Jimenez sold controlling interest of the company to James Hawkins. Mr. Jimenez currently owns 9 percent of GovWare, LL. There is no relationship between Govware, LLC and MicroTech, LLC. Mr. Jimenez is a passive investor in Govware, LLC.

A mere two years later in 2007, Mr. Jimenez, the passive investor, would formally retake control of GovWare, and in a letter from Mr. Timothy Wharton (also a managing member of GovWare as well as a member of MicroTech and MicroLink) would inform GovWare's members that "all or substantially all" of GovWare's assets would be sold to MicroTech, a firm that SBA had been told had "no relationship" with GovWare.

In 2007, MicroTech described its acquisition of GovWare's assets, which is the company that two years earlier Mr. Jimenez and MicroTech had assured SBA had "no relationship" to MicroTech, as follows:

> On June 30, 2007, the Company [MicroTech] assumed all assets, liabilities and contract obligations of a company owned by the Company's members, GovWare, LLC (GovWare). The merger was between entities under "common control". Therefore, the assets and liabilities assumed were recorded at historical cost as if the companies were combined since inception in accordance with accounting principles generally accepted in the United States of America.
> Prior to June 30, 2007, the Company [MicroTech] and GovWare, in the normal course of business, entered into certain transactions for the purchase and sale of services. These intercompany transactions have been eliminated in the accompanying financial statements.

In statements to SBA in 2005, Mr. Jimenez maintained that he was merely a passive investor in GovWare and that the two companies had no relationship. In 2007, the firms were described as under common control and as having intercompany contracts and transactions that relate back to the inception of the firms. The two statements are not compatible. The 2005 statement had the effect of misleading SBA about the true nature of the relationship and connections between the two firms and their officers and owners. SBA was led to believe by Mr. Jimenez that the two firms would be separate, and that he and MicroTech would have "no relationship" with the firm, and this was asserted along with his statement of being just a "passive" investor.

How is it that Mr. Jimenez, and his partners in MicroTech (Mr. David Truitt and Mr. Timothy Wharton) were able to own and control GovWare in 2007 when Mr. Jimenez and MicroTech previously told SBA that Mr. Jimenez and his MicroTech partners were just passive investors and that the businesses were completely separate and had "no business relationships"? It appears that the answer is that Mr. Jimenez and MicroTech purposefully misled SBA about the relationship in 2005 and also withheld corporate documents from SBA. Specifically while Mr. Jimenez and MicroTech did provide GovWare's Operating Agreement, including amendments and updates, they failed to provide SBA with a May 31, 2005[2] Option Agreement between the

[2] MicroTech was not admitted to 8(a) program until June 10, 2005 and its application was still under review at the time the option agreement was dated. Further, even if the option agreement was dated after MicroTech had been admitted the program, the firm would have had an affirmative duty to provide SBA with a copy. "The concern must

members of GovWare. That Option Agreement was never disclosed to SBA during the review of MicroTech's application, or after the firm was accepted into the program in June 2005. The Option Agreement allowed Mr. Jimenez to "repurchase" Mr. Hawkins shares at any time for a few hundred dollars. In 2007, Mr. Jimenez exercised those options, and he and his partners then transferred all the assets of GovWare to the company that Mr. Jimenez had certified to SBA that it had no business relationships with, MicroTech. The existence of options is extremely important to SBA in evaluating ownership and control, as well as in determining affiliation for size purposes. Pursuant to SBA's regulations for its various socio-economic programs, including the 8(a) BD program, SBA will generally treat stock options as exercised in determining who controls the firm under review. *See* 13 C.F.R. § 121.103(d), § 124.105(e); § 125.9(e); § 126.201(a); and § 127.201(f). Where another individual or business entity has the authority to exercise options or convert debentures to voting stock in a firm that would affect the control of the firm (e.g., where an individual would own more than 50% of a firm after options are exercised), SBA will consider the options as already exercised and that individual or business entity will be deemed to control the firm. The rules are in place to cover the exact situation that occurred with Mr. Jimenez seizing control of GovWare. Reported equity holders and their percentages of ownership are illusionary if there are options outstanding that can be exercised at any time and effectively change the control of a firm. In this case, Mr. Jimenez held options for GovWare that would give him majority ownership and control of the firm. These options were never disclosed to SBA. Mr. Jimenez and MicroTech misled SBA about the extent and nature of the relationship between himself, MicroTech, Mr. Truitt, Mr. Wharton, and GovWare.

In addition, Mr. Jimenez, Mr. Truitt and Mr. Wharton were deemed to be the "Initial Members" of GovWare. Pursuant to GovWare's Operating Agreement, certain rights were granted exclusively to the Initial Members. Thus, even after GovWare added Mr. James Hawkins as an additional Member, Mr. Jimenez, Mr. Truitt and Mr. Wharton continued to control GovWare regarding significant actions. When Mr. Hawkins later attempted to dispute actions that eliminated his ownership interest in GovWare, he was told that as an "additional member" of GovWare, he did not have the authority to do so. Specifically, he was told that the "Right of First Refusal to Purchase Company Assets" was "solely and expressly granted to the Initial Members." *See* July 3, 2007 Letter from Patton Boggs LLP. As such, it appears that Mr. Jimenez continued to possess significant control over GovWare even after his supposed sale of his controlling interest to Mr. Hawkins in January 2005, contrary to his assertions in MicroTech's 8(a) application.

During the application process, SBA also requested information from MicroTech regarding the relationship between itself, its owners and members, and the firm MicroLink and that firm's owners and officers. In response to SBA's request, MicroTech provided the following response:

> Anthony Jimenez is the majority owner of Micro Tech, LLC, David Truitt is a minority owner in Micro Tech, LLC. Although David Truitt holds ownership in the firm, he does not hold any position within the firm. Additionally, he receives no regular salary from Micro Tech, LLC. He is not in any managerial capacity

---

inform SBA in writing of any changes in circumstances which would adversely affect its program eligibility, especially economic disadvantage and ownership and control." 13 C.F.R. § 124.112 (2005).

within the company. David Truitt is the majority shareholder of Micro Link, LLC in the capacity of CEO and President.

There is no link, relationship, or partnership of **any kind** between Micro Tech, LLC and Micro Link, LLC. Micro Tech, LLC operates in an entirely different NAICS code than Micro Link, LLC. The NAICS code that Micro Tech is operating under is 517212. Micro Link is operating under NAICS code 541511. Micro Tech, LLC is neither a vendor to nor a customer of Micro Link, LLC. **No business has ever** been conducted between these two companies. [Emphasis added.]

This is a very clear statement on the part of MicroTech that it does not do any business with MicroLink, and, given the different NAICS codes that the two companies operate in, that there is no intention of doing business together in the future. The clear intent of this statement is to lead SBA to believe that no business relationship exists now, and that no business relationship will exist in the future. That is the clear intent of the statement, and that is the meaning that SBA applied to the statement. However this statement appears to be a complete fabrication, and the future conduct of all parties now being proposed for debarment sheds light on their original motives.

MicroTech's actions after its acceptance into the 8(a) BD program paint a much different picture of the relationship between the companies and between Mr. Jimenez, Mr. Truitt, and Mr. Wharton than the one presented by the firms and Mr. Jimenez at the time of MicroTech's application. Rather than having no links, no relationships, no partnerships of any kind, and no business together ever, MicroTech reported substantial payments to MicroLink[3]. In 2005, MicroTech recorded $35,924 in rent, and $258,780 for "subcontractor, commissions, accounting, and consulting expenses" to MicroLink. In 2006, MicroTech recorded $177,626 for rent and an additional $120,658 for "subcontractor, commissions, accounting, and consulting expenses" to MicroLink. In 2007, MicroTech recorded $182,630 for rent and an additional $622,618 for "subcontractor, commissions, accounting, and consulting expenses" to MicroLink. In 2008, MicroTech recorded $353,450 for rent and an additional $529,003 for "subcontractor, commissions, accounting, and consulting expenses" to MicroLink.

MicroTech and MicroLink Transactions 2005-2008

	Rent	Subcontractor, commissions, accounting, and consulting expenses	Total
2005	$35,924	$258,780	$296,709
2006	$177,626	$120,658	$300,290
2007	$182,630	$622,618	$596,999
2008	$353,450	$529,003	$884,461
Total	$749,630	$1,531,059	$2,280,689

[3] The records being referenced do not name MicroLink, but rather state a "company owned by two of its members." With knowledge from outside those documents I am assuming this is a reference to MicroLink and not to another firm not disclosed to SBA.

In the year in which MicroTech applied to the 8(a) BD program and the following three years, MicroTech had $749,630 recorded in rent payments and $1,531,059 recorded in "subcontractor, commissions, accounting, and consulting expenses". Mr. Jimenez's and MicroTech's assertion that the two firms were separate and had no relationships is not born out by their subsequent conduct. $2,280,689 is not a small or de minimis amount of business between two firms and is a far cry from the, "no link, relationship, or partnership of any kind between Micro Tech, LLC and Micro Link, LLC" statement made to SBA.

Further, MicroTech's application and response does not state that Mr. Timothy Wharton, a member of MicroTech since its inception in 2004, also owns 20% of MicroLink, is member of both companies, and is an officer of MicroLink. Further with respect to MicroLink, LLC and Mr. Wharton, SBA's application for the 8(a) BD program asks the following the question, "Does any owner, director, officer or management member have an ownership interest in any other firm?" MicroTech's application states that the answer to that question is "yes", but only provides the name of Mr. David Truitt, and not Mr. Timothy Wharton.

The response also states that, "Although David Truitt holds ownership in the firm, he does not hold any position within the firm." Whether this was true at the time of MicroTech's application is debatable[4], but Mr. Truitt either officially or unofficially held officer titles and positions at MicroTech during the firm's participation in the 8(a) BD Program. SBA was never informed at the time that Mr. Truitt's role had changed, and that he had been made an officer of the firm as required by SBA regulations.

The record also shows that MicroTech may not have been a small business concern for many of the contracts it was awarded between 2005 and 2010[5] due to the affiliation between MicroTech and MicroLink. *See* 13 C.F.R. § 121.103. The record shows a deep and thorough connection between the two firms, its management and its owners. The firms had common ownership and management (Mr. Truitt has been shown to be listed as an officer of both firms), shared resources and were co-located at the same location. Pursuant to SBA's regulations, "SBA considers factors such as ownership, management, previous relationships with or ties to another concern, and contractual relationships, in determining whether affiliation exists." 13 C.F.R. § 121.103(a)(2). While no one factor may be dispositive, SBA regulations clearly state that, "[i]n determining whether affiliation exists, SBA will consider the totality of the circumstances, and may find affiliation even though no single factor is sufficient to constitute affiliation." § 121.103(a)(5). Although SBA did conduct several size determinations of the firm during this time period in response to protests relating to specific contracts, the issue of affiliation was not raised by the protestor and was not determined by SBA. The issue of affiliation was raised in a size determination in 2012, but at that time Mr. Wharton and Mr. Truitt no longer owned MicroLink, and Mr. Truitt was no longer working for MicroLink. In 2012, Mr. Truitt was working full time for MicroTech. However, prior to 2010 there are substantial links between the

[4] It appears that Mr. Truitt may have always held an officer title and position within the firm, but MicroTech did not view this as an officer position because Mr. Jimenez had ultimate control. At the least, SBA believes that further clarification was required because common sense would lead to a conclusion that a person with a title and a position as an officer is an officer.

[5] In 2010, MicroLink was sold to another business.

two companies, and clearly Mr. Truitt and Mr. Wharton owned significant interests in both firms, as well as GovWare. Rather than operating as two independent entities, the record appears to show a very close relationship between all parties, and separate entities owned by common individuals operating together both formally and informally. For example, when Mr. Truitt sold MicroLink, he did not go to work for another firm; he continued to work as an officer for MicroTech.

There is also an issue regarding the total amount of compensation provided by MicroTech to Mr. Jimenez and Mr. Truitt. SBA's 8(a) BD regulations require that Mr. Jimenez be the highest compensated individual in the 8(a) participant firm. *See* 13 C.F.R. § 124.106(e)(3). Records show that Mr. Truitt and Mr. Jimenez were both paid dividends by MicroTech for most years. For example, in 2007 MicroTech paid Mr. Jimenez $175,333 and Mr. Truitt $126,151 in dividends. According to records, neither drew a salary that year. However, records also show, as noted above, that MicroLink received $596,999 ($182,630 for rent and $622,618 for subcontractor, commissions, accounting, and consulting expenses) from MicroTech that year. As a principal of MicroLink, Mr. Truitt certainly received benefits from the transactions between MicroTech and MicroLink. In order for Mr. Jimenez to be the highest compensated individual in MicroTech, it is conceivable that MicroTech paid certain specified amounts to Mr. Truitt indirectly through MicroLink as "consulting services." Further, any rent that was paid by MicroTech to MicroLink that exceeded the fair market rate for MicroTech's space could also be considered as compensation paid by MicroTech to Mr. Truitt. Given the amount of money transferred between the two firms over the years, there are issues about the compensation of Mr. Jimenez relative to Mr. Truitt that needs further clarification.

Conclusion.

The proposed debarment is effective throughout the executive branch of the Federal Government and has the following consequences:

1. The names of the Microtechnologies, LLC d/b/a MicroTech (Duns: 145454182, and 078468018), and Mr. Anthony Jimenez will be published in the System for Award Management (SAM), where it will be noted that you are in an "Ineligible (Proceedings Pending)" status. SAM is available at http://www.sam.gov.

2. Microtechnologies, LLC d/b/a MicroTech (Duns: 145454182, and 078468018), and Mr. Anthony Jimenez are excluded from receiving contracts. Agencies shall not solicit offers from, award contracts to, or consent to subcontracts with you unless the agency head determines that there is a compelling reason for such action.

3. Microtechnologies, LLC d/b/a MicroTech (Duns: 145454182, and 078468018), and Mr. Anthony Jimenez are excluded from conducting business with the Government as agent or representative of other contractors.

4. Microtechnologies, LLC d/b/a MicroTech (Duns: 145454182, and 078468018), and Mr. Anthony Jimenez are excluded from acting as an individual surety.

5. Microtechnologies, LLC d/b/a MicroTech (Duns: 145454182, and 078468018), and Mr. Anthony Jimenez are excluded from participating in a Federal agency transaction that is a covered transaction, or act as a principal of a person participating in a covered transaction. The term "covered transaction" is defined in 2 C.F.R. § 180.200.

If debarment is imposed, the limitations described above will continue to apply and Microtechnologies, LLC d/b/a MicroTech (Duns: 145454182, and 078468018), and Mr. Anthony Jimenez will be identified in SAM as "Ineligible (Proceedings Completed)." If imposed, debarment will be for a period commensurate with the seriousness of the cause.

Within 30 days of receipt of this Notice, you or a representative may submit either in person or in writing, or both, information and argument in opposition to the proposed debarment. If you designate a representative to respond, please notify me in writing of the identity of the representative. The designation should specifically state the names and addresses of all individuals or companies the designee has the authority to represent in this matter.

Your submission, if any, may include specific information that raises a genuine dispute over facts material to the proposed debarment. If it is found that the information or argument submitted raises a genuine dispute over material facts, fact-finding may be conducted to determine the disputed facts.

This proposed debarment proceeding has been initiated on the basis of the administrative record. A copy of the record, except for those materials protected from disclosure, will be furnished upon request. Any written information you submit will become a part of the administrative record. Information or argument presented orally will be considered to be part of the administrative record only to the extent such information and argument is submitted in written form. The determination whether to debar you is discretionary and will be made on the basis of the administrative record, together with any written materials submitted for the record by the Government or you during the period of proposed debarment.

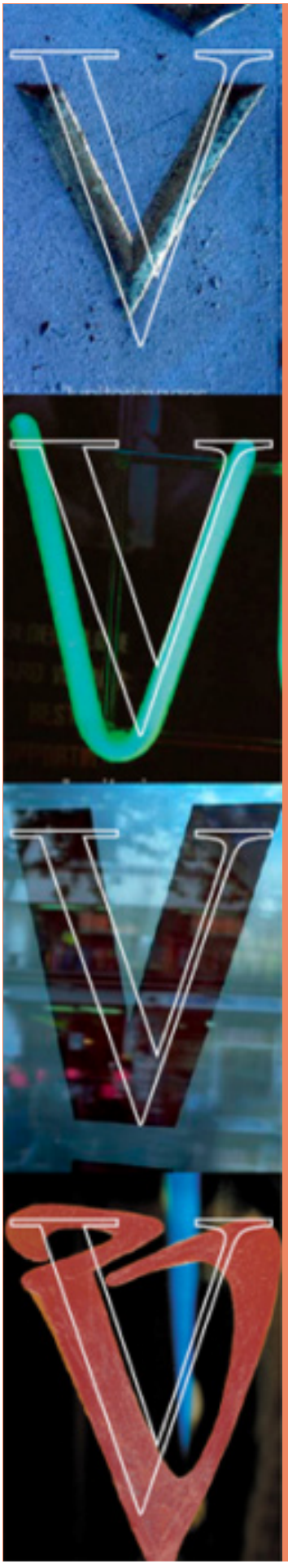
Any communications regarding this matter should be directed to Christopher Clarke of my Office at 202-205-7307. Any written submission should be forwarded to him at U.S. Small Business Administration, 409 Third Street SW, Fifth Floor, Washington, DC 20416, with a copy by email to Christopher.clarke@sba.gov.

For your information, a copy of regulations relevant to your proposed debarment are enclosed, 48 C.F.R. subpart 9.4.

Sincerely,

John W. Klein
SBA Suspension and Debarment Official

Enclosures



Protecting Against the Government's Administrative Remedies

9:50 a.m. – 10:50 a.m.

Robert A. Burton, Venable LLP

Dismas Locaria, Venable LLP

Rebecca E. Pearson, Venable LLP

Jessica Tillipman, George Washington University Law School

VENABLE® LLP

VENABLE® LLP

Protecting Against the Government's Administrative Remedies

April 10, 2014

VENABLE® LLP

Panelist Biographies

Robert A. Burton, Venable LLP - Moderator

A thirty-year veteran of procurement law and policy development, Mr. Burton served in the Executive Office of the President as Deputy Administrator of the Office of Federal Procurement Policy (OFPP), the nation's top career federal procurement official. He also served as Acting Administrator for two years during his seven-year tenure at OFPP.

As Deputy Administrator of OFPP, Mr. Burton was responsible for the government's acquisition policy and procurement guidance for all Executive Branch agencies.

His office was charged with developing policy affecting more than $400 billion in annual federal spending – a figure that doubled during Mr. Burton's time in office as a result of the Iraq War and other major events.

At OFPP, Mr. Burton was instrumental on a number of fronts, including preparing the Administration's policy positions and testimony on proposed acquisition legislation; working with House and Senate committees on the development of acquisition reform proposals; and serving as a principal spokesperson for government-wide acquisition initiatives. He also served as the Executive Director of the Chief Acquisition Officers (CAO) Council, which comprises the Chief Acquisition Officers from each federal agency. Mr. Burton also managed the activities of the Federal Acquisition Regulatory (FAR) Council, which has statutory authority to promulgate the government's procurement regulations.

Prior to joining OFPP in 2001, Mr. Burton spent over twenty years as a senior acquisition attorney with the Department of Defense. At the Defense Contract Management Agency, he negotiated the resolution of high-profile contract disputes with major defense contractors and provided advice on cost allowability issues. He served as general counsel for DoD's Defense Energy Support Center, as well as associate general counsel for the Defense Logistics Agency (DLA), the DoD component responsible for purchasing most of the general supplies and services used by the military services. At DLA, Mr. Burton served as counsel to the agency's suspension and debarment official and managed the agency's fraud remedies program, working with the Department of Justice and the criminal investigative agencies to coordinate appropriate remedies in major procurement fraud cases.

Panelist Biographies

Jessica Tillipman, George Washington University Law School

Jessica Tillipman is the Assistant Dean for Field Placement and Professorial Lecturer in Law at George Washington University Law School. In addition to managing the law school's large externship program, she teaches a Government Contracts Anti-Corruption & Compliance Seminar that focuses on corruption control issues in government procurement. She also advises companies on anti-corruption compliance issues.

Prior to joining GW, Dean Tillipman was an associate in Jenner & Block's Washington, DC office, where she was a member of the firm's Government Contracts and White Collar Criminal Defense and Counseling practice groups. She joined Jenner & Block after serving as a law clerk to the Honorable Lawrence S. Margolis of the U.S. Court of Federal Claims.

Dean Tillipman is a Senior Editor of *The FCPA Blog*—a leading Foreign Corrupt Practices Act resource on the internet. She has also published articles on various government contracts and white collar topics, including the Foreign Corrupt Practices Act, suspension and debarment, and government ethics in T*he George Washington University International Law Review*, *Fordham Law Review Res Gestae*, the *Public Contract Law Journal*, *Public Procurement Law Review*, and Thomson Reuters' *Briefing Papers*. Her forthcoming article, "Gifts, Hospitality and the Government Contractor," will be published by Thomson Reuter's *Briefing Papers* in April 2014. Dean Tillipman graduated cum laude from Miami University in Oxford, Ohio and obtained her JD, with honors, from George Washington University Law School.

Panelist Biographies

Dismas (Diz) N. Locaria, Venable LLP

Dismas (Diz) Locaria is a member of the firm's Government Contracts Group. Mr. Locaria's practice focuses on assisting government contractors in all aspects of working with the federal government, as well as representing and counseling clients concerning the peculiarities of the Homeland Security Act's SAFETY Act.

Mr. Locaria has represented clients before various federal agencies, including the Department of Defense, General Services Administration, Department of Homeland Security, Small Business Administration, Environmental Protection Agency, and others. Mr. Locaria has developed several specialty areas, including representing clients in suspension and debarment proceedings, as well as performing internal investigations, which has included assistance and representation for such clients with disclosures to federal officials regarding the findings of such investigations and working with the client to determine and implement compliance enhancements and improvements. Mr. Locaria also has extensive experience in client counseling, including assisting clients with the nuances of becoming government contractors and implementing appropriate systems and methods to achieve and maintain regulatory and contractual compliance. Mr. Locaria is also well versed in assisting clients with GSA Federal Supply Schedule matters, particularly advising clients on how best to structure proposals to avoid price reduction clause (PRC) issues, and addressing PRC, Trade Agreements Act and other compliance matters post-award.

Panelist Biographies

Rebecca E. Pearson, Venable LLP

Rebecca Pearson focuses on government contracts law. She assists clients in government contract litigation; contract award protests before the Government Accountability Office and federal courts; administrative claims before agency boards of contract appeals; representation before the Department of Justice and federal courts on civil matters involving government contractors; and civil litigation in federal courts involving government prime contractors and subcontractors. Ms. Pearson also counsels clients on matters involving contracts including defective pricing and cost allowance questions, teaming agreements, legal and regulatory compliance and ethics, and small business issues. She has significant experience with due diligence in connection with the merger and acquisition of government contractors, as well as post-transaction matters such as novation.

Ms. Pearson's extensive experience as an Air Force attorney in federal litigation and client counseling, and in interfacing with other federal agencies, provides her with an invaluable "insider's" perspective and proven skills to render timely and effective assistance to clients in a wide variety of government contracts matters.

Agenda

- The Suspension and Debarment Bubble
- Legislative Developments (past & present)
- BP Suspension and Administrative Agreement
- The *Agility Defense* Case
- The Onslaught of Fact-Based Debarments – Fair or Foul
- Practitioner's Points

VENABLE LLP

The Suspension & Debarment Bubble

- Spurred by the Clean Contracting Act, few areas of enforcement are on the rise like suspension and debarment:

	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
AIR FORCE					
Suspensions	73	91	148	83	42
Proposed Debarments	86	68	139	**401**	**205**
Debarments	63	206	80	**266**	185
ARMY					
Suspensions	134	133	112	**195**	71
Proposed Debarments	112	125	**235**	**284**	**316**
Debarments	117	170	179	186	**258**
NAVY					
Suspensions	12	25	24	47	**137**
Proposed Debarments	39	38	80	**152**	**189**
Debarments	44	78	92	**146**	109
DEFENSE LOGISTICS AGENCY					
Suspensions	48	141	34	18	18
Proposed Debarments	163	166	**212**	**179**	**190**
Debarments	131	169	**190**	**202**	167

VENABLE LLP

Legislative Developments

- Legislative developments are troubling and signal that the bubble will likely grow:
  - Clean Contracting Act of 2010
    - Required agencies to report S&D activity to Congress
  - Consolidated Appropriations Act of FY12 included an ineligibility provision for felons
  - Remained in FY13 and FY14 appropriations
  - SUSPEND Act – Creating a quasi-judicial system

BP Suspension and Administrative Agreement

- BP suspended from federal contracting in November 2012, two years after the Deepwater Horizon spill
  - Protection of public interest vs. punishment of contractors
- BP entered into an administrative agreement with EPA in March 2013, which lifted the suspension
  - Ethics and safety monitoring provisions
  - EPA-approved auditor

Agility Defense & Government Services, Inc. v. U.S. Department of Defense

- *Agility Defense* Case
  - Issue: Whether an agency must initiate legal proceedings against an affiliate of an indicted government contractor to toll the 18-month limit on the suspension of the affiliate, even though the affiliate was suspended solely because of its affiliate status
  - District Court (No. CV-11-S-4111-NE, (N.D. Ala. Jun. 26, 2012)) held:
    - Government may suspend an entity based on its affiliation
    - Cannot suspend indefinitely without initiating a "legal proceeding" against the affiliate
  - The 11th Cir. (No. 13-10757 (Dec. 31, 2013)) reversed, allowing agencies to indefinitely suspend affiliates of an indicted government contractor

Background

- The FAR defines "affiliates" as:

  Business concerns, organizations, or individuals are affiliates of each other if, directly or indirectly, (1) either one controls or has the power to control the other, or (2) a third party controls or has the power to control both.

- FAR 9.407-1 provides:

  The ***suspending official may extend the suspension decision to include any affiliates*** of the contractor if they are (1) specifically named and (2) given written notice of the suspension and an opportunity to respond.

- FAR 9.407-4(b) provides:

  If legal proceedings are not initiated within 12 months after the date of the suspension notice, the suspension shall be terminated unless an Assistant Attorney General requests its extension, in which case it may be extended for an additional 6 months. ***In no event may a suspension extend beyond 18 months, unless legal proceedings have been initiated within that period.***

The 11th Circuit's Decision

- The Eleventh Circuit made two holdings:

1. The term "legal proceedings" referred to proceedings against the indicted government contractor, not the affiliate.
   - FAR 9.407-1 made "clear that the suspension and debarment of an affiliate derive solely from its status as an affiliate," irrespective of whether there has been a showing of wrongdoing by the affiliate.
   - To suspend an affiliate, an agency must satisfy three requirements:
     (1) establish that the affiliate has the power to control, or be controlled by, the indicted government contractor
     (2) specifically name the affiliate
     (3) provide notice of the suspension and notice of an opportunity for the affiliate to respond

The 11th Circuit's Decision (cont'd)

2. The suspension of an affiliate for more than 18 months does not violate the affiliate's right of due process under the Fifth Amendment.
   - "It is unlikely that the regulation infringes on the liberty interests of the affiliates given that their suspensions were predicated solely on their status as affiliates of [the indicted government contractor] and the agency did not make any allegations of wrongdoing against them."
   - "[T]he regulation does not violate the Due Process Clause because it contains constitutionally adequate procedures[,]" specifically, notice and an opportunity to respond in writing.

- March 31, 2014 – Agility's petition for an *en banc* rehearing denied

Concerns with the *Agility Defense* Decision

- The court stated:
  - "The United States and its agencies have little reason to initiate legal proceedings against an affiliate suspended solely on account of its affiliate status."
  - The court came to this conclusion because "[t]he present responsibility of an affiliate is irrelevant."
- FAR 9.4 is completely predicated on present responsibility; 11th Cir. tosses this aside.
- Suspension/debarment are not for punishment and not to be taken lightly
  - Decision allows for a no-analysis determination based on affiliation
  - Renders opportunity to respond meaningless

Concerns with the *Agility Defense* Decision (cont'd)

- If ability to respond is meaningless, how is liberty interest protected?
- Worse yet, 11th Cir. is *not even* certain that liberty interests are protected:

  "It is *unlikely* that the regulation infringes on the liberty interests of the affiliates…"

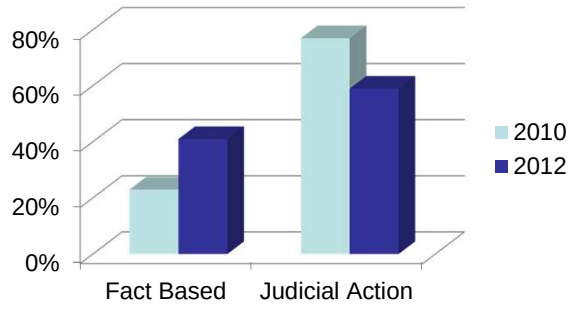
What to Do

- If you are an affiliate organization
  - Must keep up with integrity conduct and issues of parent and affiliates
  - If issues arise, must take proactive steps:
    - Assure agencies that there is no need to suspend or propose for debarment
    - Establish independence from offending parent and/or affiliate
- Closely held companies where owner(s) are implicated in wrongdoing
  - Company likely deemed affiliated
  - Divest control

Fact-based suspension and debarments

- A “fact-based” suspension is an action based entirely on the strength of the facts absent a predicate judicial or administrative finding, such as an indictment.
- Suspensions without legal proceedings are limited to 12 months, plus a 6-month extension.

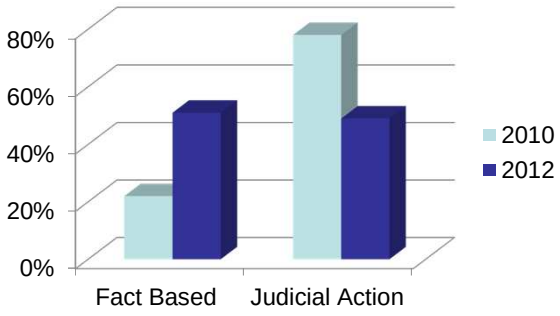
Fact-Based Suspension Referrals Are on the Rise



	2010	2012
Fact Based	23%	**41%**
Judicial Action	77%	**59%**

VENABLE LLP

Fact-Based Debarments Referrals Are on the Rise



	2010	2012
Fact Based	22%	**51%**
Judicial Action	78%	**49%**

VENABLE LLP

Causes of Rise in Fact-Based Actions

- Increased coordination among agency personnel

OIG | Auditor | Inspector

Evaluator | SDO | CO

Program Manager | Special Agents | COTR

Causes of Rise in Fact-Based Actions (cont'd)

- Data mining by agencies of top news stories
- Increased breadth and number of civil false claims actions

Causes of Rise in Fact-Based Actions (cont'd)

- Congressional scrutiny of agency administrative action and failure to act
- Increased action pursuant to "any other case of so serious or compelling a nature that it affects the present responsibility of the contractor"

VENABLE LLP

Fair or Foul?

Fair

- In certain cases, agencies may need to protect themselves prior to an indictment or final finding of liability

Foul

- Increases costs of defending against alleged misconduct
- Agencies' procedures may not provide due process
- Motivation?
  - Statistics alone (improper)
  - Protection (proper)

VENABLE LLP

What to Do
Be Proactive

- Have an ethics and compliance program, even if you are a small business.
- If misconduct occurs, determine whether disclosure is mandatory or appropriate.
- Engage the SDO early where appropriate.

VENABLE LLP

Contact Information

YOUR VENABLE TEAM

Robert A. Burton
rburton@Venable.com
t 202.344.4776
f 202.344.8300

Rebecca E. Pearson
repearson@Venable.com
t 202.344.8183
f 202.344.8300

Dismas (Diz) N. Locaria
dlocaria@Venable.com
t 202.344.8013
f 202.344.8300

www.Venable.com

Additional Information

BP Administrative Agreement

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

BEFORE THE UNITED STATES ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF ADMINISTRATION AND RESOURCES MANAGEMENT

In the matter of:	)	
	)	
BP p.l.c.	)	EPA Case No. 12-0295-00
BP America, Inc.	)	EPA Case No. 12-0295-02
BP Exploration and Production Inc.	)	EPA Case No. 12-0295-05
BP Products North America, Inc.	)	EPA Case No. 12-0295-06
BP Exploration (Alaska), Inc.	)	EPA Case No. 12-0295-19

ADMINISTRATIVE AGREEMENT

I. INTRODUCTION

This Administrative Agreement ("Agreement") is made between the United States Environmental Protection Agency ("EPA"), acting as lead federal agency, and: BP p.l.c.; BP America, Inc. ("BPA"); BP Exploration and Production Inc. ("BPXP"); BP Products North America, Inc. ("BPPNA"); BP Exploration (Alaska), Inc. ("BPXA"); and other BP Group Entities as set forth herein. For purposes of this Agreement, unless otherwise stated herein, BP Group Entities groupings are designated as set forth in Section II below, and the provisions of this Agreement specifically applicable to these respective groupings are set forth in Section IV herein.

This Agreement resolves all administrative matters relating to suspension and debarment and statutory disqualification, and any suspension and debarment matter based on affiliation or imputation, arising from:

A. BPXP's January 29, 2013 conviction for violating the Clean Water Act ("CWA"), eleven (11) counts of Seaman's Manslaughter, violating the Migratory Bird Treaty Act ("MBTA") and Obstruction of Congress;

B. BP p.l.c.'s December 10, 2012 Securities Exchange Commission ("SEC") Judgment Order;

C. BPXA's November 29, 2007 conviction for violating the CWA; and

D. BPPNA's March 12, 2009 conviction for violating the Clean Air Act ("CAA").

II. DEFINITIONS

AGENTS. Shall mean any person(s) as defined by 2 C.F.R. § 180.985, who act(s) on behalf of or who is authorized by a BP Covered Entity to commit the BP Covered Entity in a business transaction in the United States ("U.S.").

AFFILIATES. As defined in 2 C.F.R. § 180.905, an Affiliate to BP p.l.c. is any entity that directly or indirectly controls or is controlled, or has the power to control or be controlled by BP p.l.c. In addition, an Affiliate to BP p.l.c. is any entity that is controlled by the same third party as BP p.l.c. Indicia of control include, but are not limited to: (a) interlocking management or ownership; (b) identity of interests among family members; (c) shared facilities and equipment; (d) common use of employees; or (e) a business entity which has been organized following the exclusion of a person which has the same or similar management, ownership or principal employees as the excluded person. Affiliates shall not include joint ventures.

ARM'S LENGTH TRANSACTION. Shall mean a bona fide transaction between a purchaser and a seller, each acting independently and having no Affiliate relationship with a BP Group Entity. Both parties in the transaction are acting in their own self-interest and are not subject to any duress from the other party.

BP GROUP ENTITIES. Shall be used as the generic title for BP p.l.c. and the entirety of Affiliates, subsidiaries, operations, etc. ultimately overseen by BP p.l.c.

BP AFFILIATES WITH FOREIGN BUSINESS. Shall mean a BP Group Entity that is not currently a Respondent or Group US Business but that enters into or is currently a party to a contract with or award by the U.S. under (a) a Federal Government procurement, or (b) nonprocurement transaction in excess of five hundred thousand dollars ($500,000.00), the performance of which will occur outside the U.S. during the term of this Agreement.

BP COVERED ENTITIES. Shall mean Respondents, Group US Businesses, Covered Affiliates and BP Affiliates with Foreign Business.

BP SENIOR LEVEL LEADER. Shall mean BP Covered Entity Employees at Level "F" and above.

BP'S AUTHORIZED REPRESENTATIVE(S). Shall mean the primary contact(s) for BP Covered Entities for the purpose of this Agreement. That person(s) is listed at paragraph 31 of Section XII (General Provisions) herein. All matters involving this Agreement shall be coordinated through this person(s), including but not limited to questions, requests and other communications.

BPXP/BPXA ENTITIES. For the purposes of Section IX (Process Safety), BPXP/BPXA Entities shall mean BPXP, BPXA and any Affiliates participating in activities in the waters of the U.S.

CONTRACTOR. Shall mean any individual or other legal entity, other than an Employee of a BP Covered Entity or Contract Personnel, with whom a BP Covered Entity has a primary mutually binding legal relationship or contract to conduct business or provide goods or services in the U.S., or to conduct business or provide goods or services on projects under Federal Government procurement or nonprocurement awards worldwide. Contractors shall not be considered Contract Personnel.

CONTRACT PERSONNEL. Shall mean administrative staff of an organization other than a BP Covered Entity (who is thus subject to that organization's salary and benefits structure), provided that organization sells the employee's services to a BP Covered Entity on a project or time basis.

COVERED AFFILIATES. Shall mean: BP America Production Company; BP Corporation North America Inc.; BP Oil International Limited; Air BP Limited; BP Marine Limited; BP West Coast Products LLC; BP Singapore; BP Australia PTY Limited; BP Marine Global Investments Salah Company LLC; BP Energy Company; Atlantic Richfield Company; BP Amoco Chemical Company; BP Company North America Inc.; Standard Oil; BP International Limited; BP Marine Americas; IGI Resources, Inc.; Castrol Marine Americas; BP Alternative Energy; and BP Pipelines (Alaska), Inc.

EMPLOYEES. Shall mean any natural person hired directly by a BP Covered Entity in an employer-employee relationship (and thus subject to the BP Covered Entity's salary and benefits structure) to provide labor or services to the BP Covered Entity. The term includes temporary, full-time or part-time employees who meet the criteria of the preceding sentence, and "Principal," as defined below.

EPA AUTHORIZED REPRESENTATIVE(S). Shall mean the EPA official(s) who is the primary EPA contact(s) for the purpose of this Agreement. That person(s) is listed at paragraph 31 of Section XII (General Provisions) herein. All matters involving this Agreement shall be coordinated through this person(s), including but not limited to questions, submittals and other communications.

EPA INDEPENDENT AUDITOR. Shall mean the auditor responsible for reviewing and reporting on the BP Covered Entities' compliance with this Agreement. Specific duties and responsibilities of the EPA Independent Auditor, and the BP Covered Entities' obligations with respect to the EPA Independent Auditor, are further set forth herein.

ETHICS MONITOR. Shall mean the "Ethics Monitor" set forth in Exhibit B of the January 29, 2013 Plea Agreement in *United States v. BP Exploration and Production, Inc.*, 2:12-CR-00292-SSV-DEK (E.D. La.). Specific duties and requirements of the Ethics Monitor and obligations are set forth in the Remedial Order and in this Agreement.

FEDERAL GOVERNMENT. Shall mean any department, agency, division or independent establishment of the Executive Branch of the federal government of the U.S.

GOVERNMENT ENTITY(IES). Shall mean all U.S. federal, state, commonwealth, territory and local governments, including the governments of the District of Columbia, the Commonwealth of Puerto Rico and other U.S. territories or possessions.

GROUP US BUSINESSES. Shall mean BPA and its affiliates, or any successors of BPA and its affiliates, to the extent that their operations are in the U.S. or the waters of the U.S., as well as other BP Group Entities to the extent that they, during the term of this Agreement, conduct substantial operations in the U.S. or waters of the U.S.

GROUP US EMPLOYEES. Shall mean all Employees of Group US Businesses who perform duties in the U.S., including any Employees seconded to joint ventures in the U.S.

PERIOD OF TIME. The number of days referenced in this Agreement shall be calculated by calendar days, inclusive of all weekdays, weekends and holidays.

PRINCIPAL. Shall be defined as set forth in 2 C.F.R. § 180.995 and 48 C.F.R. § 2.101(b). The term Principal includes BP Covered Entities' BP Senior Level Leaders.

PROCESS SAFETY MONITOR. Shall mean the "Process Safety Monitor" set forth in Exhibit B of the January 29, 2013 Plea Agreement in *United States v. BP Exploration and Production, Inc.*, 2:12-CR-00292-SSV-DEK (E.D. La.). Specific duties and requirements of the Process Safety Monitor are set forth in the Remedial Order.

RESPONDENTS. Shall mean BP p.l.c., BPA, BPXP, BPPNA and BPXA.

THIRD-PARTY AUDITOR. Shall mean the "Third-Party Auditor" set forth in Exhibit B of the January 29, 2013 Plea Agreement in *United States v. BP Exploration and Production, Inc.*, 2:12-CR-00292-SSV-DEK (E.D. La.). Specific duties and requirements of the Third-Party Auditor are set forth in the April 19, 2013 Implementation Plan.

US RESPONDENTS. Shall mean BPA, BPXP, BPPNA and BPXA.

III. RECITALS

A. Prudhoe Bay, Alaska

1. On or about October 24, 2007, the U.S. Attorney for the District of Alaska filed a Criminal Information in the U.S. District Court for the District of Alaska charging BPXA with one (1) count of violating the CWA in connection with two (2) 2006 oil spills. ***See* Attachment 1 (Information, *U.S. v. BP Exploration (Alaska), Inc.*).**

2. On or about October 25, 2007, BPXA entered into a Plea Agreement ("Alaska Plea Agreement") with the U.S. Attorney for the District of Alaska, under which BPXA was required to:

a. Plead guilty to the aforementioned CWA charge;

b. Pay a fine, restitution and community service payment totaling $20 million; and

c. Serve a three-year term of probation.

***See* Attachment 2 (Plea Agreement, *U.S. v. BP Exploration (Alaska)*).**

3. On or about November 29, 2007, the U.S. District Court for the District of Alaska entered judgment against BPXA according to the terms of the Alaska Plea Agreement. ***See* Attachment 3 (Judgment, *U.S. v. BP Exploration (Alaska)*).**

4. On or about February 26, 2008, the EPA Suspension and Debarment Official ("EPA SDO") issued a Notice of Statutory Disqualification to BPXA based on BPXA's November 29, 2007 conviction for violating the CWA (Violating Facility – Prudhoe Bay, Alaska Facility). ***See* Attachment 4 (February 26, 2008 Notice of Statutory Disqualification).**

5. On or about December 27, 2011, BPXA completed its term of probation under the Alaska Plea Agreement and fulfilled its obligations thereunder. ***See* Attachment 5 (District Court Opinion).**

B. Texas City, Texas

1. On October 22, 2007, the U.S. Attorney for the Southern District of Texas filed a Criminal Information in the U.S. District Court for the Southern District of Texas (Houston Division) charging BPPNA with one (1) felony count of violating the CAA in connection with the March 23, 2005 release and explosion at BPPNA's Texas City, Texas refinery ("Texas City Refinery"). ***See* Attachment 6 (Information, *U.S. v. BP Products North America, Inc.*).**

2. On March 12, 2009, BPPNA entered into a Plea Agreement ("Texas Plea Agreement") with the U.S. Attorney for the Southern District of Texas, under which BPPNA was required to:

a. Plead guilty to the aforementioned CAA charge;

b. Pay a fine of $50 million; and

c. Serve a three year term of probation, during which it would comply with the terms of a Settlement Agreement executed between BPPNA and the U.S. Occupational Health and Safety Administration ("OSHA").

***See* Attachment 7 (Plea Agreement, *U.S. v. BP Products North America, Inc.*).**

3. On March 12, 2009, the U.S. District Court for the Southern District of Texas (Houston Division) issued a Memorandum and Order accepting the Texas Plea Agreement and entering judgment against BPPNA according to the terms of that Agreement. ***See* Attachment 8**

(Memorandum and Order, *U.S. v. BP Products North America, Inc.*); *see also* Attachment 9 (Judgment, *U.S. v. BP Products North America, Inc.*).

4. On or about March 20, 2009, the EPA SDO issued a Notice of Statutory Disqualification to BPPNA based on BPPNA's March 12, 2009 conviction for violating the CAA (Violating Facility – Texas City, Texas Refinery). ***See* Attachment 10 (March 20, 2009 Notice of Statutory Disqualification).**

5. On or about March 12, 2012, BPPNA completed its term of probation under the Texas Plea Agreement. ***See* Attachment 11 (Termination of supervision letter).**

6. On or about February 1, 2013, BPPNA sold the Texas City Refinery to Marathon Petroleum Corporation. ***See* Attachment 12 (Texas City Refinery Sale Notice).**

C. ***Deepwater Horizon***

1. On or about April 20, 2010, the Macondo Well which was being temporarily abandoned by the *Deepwater Horizon* blew out. The blowout resulted in multiple explosions and the release of oil into the Gulf of Mexico. On or about July 16, 2012, the BP Group Entities submitted a Present Responsibility Presentation to the EPA SDO ("July 16, 2012 PRP"). ***See* Attachment 13 (BP July 2012 Present Responsibility Submission).**

2. On November 14, 2012, the Federal Government filed a Superseding Indictment in the U.S. District Court for the Eastern District of Louisiana, charging both Robert Kaluza and Donald Vidrine with eleven (11) counts of Involuntary Manslaughter, eleven (11) counts of Seaman's Manslaughter and one (1) count of violating the CWA. ***See* Attachment 14 (Superseding Indictment, *U.S. v. Robert Kaluza and Donald Vidrine*).**

3. On November 14, 2012, the U.S. Department of Justice ("DOJ") filed an Indictment in the U.S. District Court for the Eastern District of Louisiana charging David Rainey with one (1) count of Obstruction of Congress and one (1) count of making False Statements. ***See* Attachment 15 (Indictment, *U.S. v. David Rainey*).**

4. On November 15, 2012, the U.S. Attorney for the Eastern District of Louisiana and the Assistant Attorney General for the Criminal Division of DOJ filed a Plea Agreement and Information in the U.S. District Court for the Eastern District of Louisiana, charging BPXP with eleven (11) counts of Seaman's Manslaughter, one (1) count of violating the CWA, one (1) count of violating the MBTA and one (1) count of Obstruction of Congress in connection with the April 20, 2010 *Deepwater Horizon* explosion, oil spill and response. ***See* Attachment 16 (November 15, 2012 Plea Agreement and Information).**

5. On November 23, 2012, the EPA Suspension and Debarment Division ("EPA SDD") submitted a November 23, 2012 Revised Action Referral Memorandum ("ARM") to the EPA SDO recommending that all Respondents and Covered Affiliates—except for Castrol Marine Americas, BP Alternative Energy and BP Pipelines Alaska—be suspended. The November 23, 2012 ARM is attached hereto. ***See* Attachment 17 (Revised ARM re: BP).**

6. On November 28, 2012, the EPA SDO issued a Notice of Suspension to all Respondents and Covered Affiliates—except for Castrol Marine Americas, BP Alternative Energy and BP Pipelines Alaska—based, in part, on criminal charges filed against BPXP on November 15, 2012. ***See*** **Attachment 18 (Notice of Suspension re: BP).**

7. On December 10, 2012, the U.S. District Court for the Eastern District of Louisiana entered a civil "Final Judgment as to Defendant, BP p.l.c." ***See*** **Attachment 19 (SEC Final Judgment Order).**

8. On January 4, 2013, in response to EPA SDD's January 4, 2013 Supplemental ARM, the EPA SDO issued a Notice of Suspension to Castrol Marine Americas. ***See*** **Attachment 20 (Supplemental ARM re: Castrol Marine Americas).**

9. On January 29, 2013, the U.S. District Court for the Eastern District of Louisiana accepted the Plea Agreement between the U.S. and BPXP, and BPXP was convicted of eleven (11) counts of Seaman's Manslaughter, one (1) count of violating the CWA, one (1) count of violating the MBTA and one (1) count of Obstruction of Congress. ***See*** **Attachment 21 (Judgment, *U.S. v. BP Exploration and Production, Inc.*); *see also* Attachment 22 (April 19, 2013 Implementation Plan).**

10. On February 1, 2013, the EPA SDO issued a Notice of Statutory Disqualification to BPXP based on BPXP's January 29, 2013 conviction for violating the CWA. ***See*** **Attachment 23 (February 1, 2013 Notice of Statutory Disqualification).**

11. On February 15, 2013, the Respondents and Covered Affiliates submitted their opposition to the November 28, 2012 Notice of Suspension and the EPA SDO's February 1, 2013 Notice of Statutory Disqualification. ***See*** **Attachment 24 (BP's February 15, 2013 Presentation of Matters in Opposition).**

12. On July 19, 2013, after additional submissions were made by the parties, the EPA SDO issued his decision continuing the suspensions. ***See*** **Attachment 25 (EPA SDO's July 19, 2013 Written Decision).**

13. On August 12, 2013, Respondents and Covered Affiliates filed a Complaint for Declaratory and Injunctive Relief in the U.S. District Court for the Southern District of Texas in which Respondents and Covered Affiliates challenge EPA's November 28, 2012 and January 4, 2013 suspension actions and EPA's February 1, 2013 statutory disqualification action. ***See*** **Attachment 26 (BP's August 12, 2013 Complaint).**

14. On November 22, 2013, EPA SDD submitted a second Revised Action Referral Memorandum and Exhibits (collectively, "November 22, 2013 ARM") to the EPA SDO recommending the continued suspension and proposed debarment of Respondents and Covered Affiliates. ***See*** **Attachment 27 (November 22, 2013 ARM).**

15. On November 26, 2013, the EPA SDO issued a Notice of Continued Suspension and Proposed Debarment to Respondents and Covered Affiliates. ***See* Attachment 28 (November 26, 2013 Notice of Continued Suspension).**

NOW WHEREFORE,

Recognizing the information described above is grounds for debarment as it raises issues concerning the BP Covered Entities' present responsibility as Federal Government contractors, and nonprocurement transaction participants;

ensuring the integrity of procurement and nonprocurement programs of the EPA and other federal agencies; and

resolving all issues of discretionary and statutory suspension and debarment pursuant to 48 C.F.R. Subpart 9.4 and 2 C.F.R. Part 180, 33 U.S.C. §1368(a), and 42 U.S.C. §7606(a) that arise from said criminal convictions;

BP Covered Entities agree as follows:

IV. SCOPE AND APPLICATION

1. Role of BP p.l.c. To the extent expressly set forth in the following enumerated paragraphs, paragraph 2 of Section V (Compliance with Other Agreements); paragraphs 1-3, 5A, 5C, 7C, 10A, 11 and 14 of Section VII (Ethics & Compliance); Section VIII (Corporate Governance); paragraph 8 of Section IX (Process Safety); Section X (BP Covered Entities' Annual Reports); and all paragraphs of Section XII (General Provisions) except paragraphs 6 and 12, apply to BP p.l.c. In addition to the specific obligations set forth in this Agreement for BP p.l.c., BP p.l.c., as guarantor of this Agreement, shall: (a) irrevocably guarantee that, in the event of any failure of the BP Covered Entities to meet their obligations under this Agreement, BP p.l.c. will cause the BP Covered Entities to meet such obligations; (b) irrevocably commit that it will comply, and will cause each of the BP Covered Entities to comply, with the terms of this Agreement; and (c) consent to the jurisdiction of the U.S. courts solely for purposes of resolving issues with this Agreement.

2. Role of Group US Businesses. Except for those obligations in this Agreement that are specifically assigned or limited to other BP Covered Entities, such as certain provisions under Section VIII (Corporate Governance) and Section IX (Process Safety), the provisions of this Agreement apply to Group US Businesses and Group US Employees.

3. Role of BP Affiliates With Foreign Business. Provisions set forth at paragraphs 5A, 5C, 8A, 8C and 11 of Section VII (Ethics & Compliance) of this Agreement, and all paragraphs of Section XII (General Provisions), except paragraphs 6 and 12, apply to BP Affiliates with Foreign Business and to the Employees of the particular BP Affiliate with Foreign Business to the extent expressly set forth in those enumerated paragraphs.

4. Election of BP Affiliates With Foreign Business. A BP Affiliate with Foreign Business that is also a Covered Affiliate that determines not to implement the terms of this Agreement applicable to BP Affiliates with Foreign Business shall send written notice to the EPA Authorized Representative(s) and the BP Authorized Representative(s) within ninety (90) days of the Effective Date of this Agreement, and to the EPA Independent Auditor upon retention. Upon such notice, the BP Affiliate with Foreign Business shall forego participating in covered procurement or nonprocurement transactions with the Federal Government during the term of this Agreement, and shall promptly enter into a voluntary exclusion agreement in the form attached as Attachment 29. The terms and obligations of this Agreement shall no longer apply to the BP Affiliate with Foreign Business and such entity shall not be considered a party to this Agreement.

5. Election of BP Group Entities to Become BP Affiliates with Foreign Business. A BP Group Entity which is not currently a BP Covered Entity but which enters into a contract with or award by the U.S. under (a) a Federal Government procurement transaction, or (b) Federal Government nonprocurement transaction in excess of five hundred thousand dollars ($500,000.00), the performance of which will occur outside the U.S. during the term of this Agreement, shall become a BP Affiliate with Foreign Business upon the effective date of the contract. Any such entity shall send written notice to the EPA Authorized Representative(s), the EPA Independent Auditor and the BP Authorized Representative(s) by electronic mail and certified mail or equivalent within sixty (60) days of entering into such contract. The written notice shall be signed by an authorized BP Group Entity officer stating that the BP Group Entity has a copy of this Agreement and agrees to be bound by it. Such notice shall become an addendum to this Agreement.

V. COMPLIANCE WITH OTHER AGREEMENTS

1. COMPLIANCE WITH THE TERMS OF PROBATION

BPXP shall comply in full with the terms and conditions of probation ("Terms of Probation") imposed upon it by the U.S. District Court for the Eastern District of Louisiana at sentencing in the matter of *United States v. BP Exploration and Production, Inc.*, 2:12-CR-00292-SSV-DEK (E.D. La.), and entered by the Court on January 29, 2013. The Terms of Probation address deepwater drilling operations, process safety, Ethics & Compliance and other matters as set forth in the Remedial Order (Exhibit B of the Plea Agreement), and the Implementation Plan, as approved by DOJ and the Probation Officer as of April 19, 2013. Unless modified by the Court, the period of probation extends for five (5) years after entry of the Remedial Order. The Plea Agreement, Remedial Order, Implementation Plan and Judgment in the Criminal Case are attached hereto and hereby incorporated by reference as if restated in full.

A. The Remedial Order and Implementation Plan are applicable to BPXP, and its affiliates, controlled directly or indirectly by BP p.l.c., that participate in deepwater drilling operations in the Gulf of Mexico, whether such entity is in existence now or in the future.

B. Compliance with the Implementation Plan's provisions is a special condition of

BPXP's probation. As set forth in the Remedial Order and Implementation Plan, BPXP is required to provide prompt notice to the Probation Officer and DOJ of its failure to comply with any of the provisions of the Implementation Plan, including meeting any of the interim milestones, and to submit a proposal for corrective action. As specified in the Implementation Plan, failure to comply with the Implementation Plan may be grounds for the revocation or modification of BPXP's probation. (*See* Implementation Plan, Non-compliance, Paragraph G.)

C. BPXP shall implement those final recommendations or corrective action plans (after any dispute resolution process) resulting from the work of the Ethics Monitor, Process Safety Monitor or Third-Party Auditor under the Remedial Order, and progress on the implementation of any such recommendations or corrective action plans shall be reported pursuant to the Remedial Order.

D. BPXP shall submit to the EPA Authorized Representative(s) and EPA Independent Auditor any correspondence BPXP is required to submit to the U.S. as described in the DOJ-approved Implementation Plan, including prompt notice of non-compliance with the Implementation Plan and its proposal for corrective action.

E. BPXP shall notify the EPA Authorized Representative(s) and EPA Independent Auditor within ten (10) days of BPXP's discovery of any violation of the Terms of Probation or the Implementation Plan as well as any failure to comply with the Terms of Probation, Remedial Order or Implementation Plan identified by the Third-Party Auditor, Process Safety Monitor or Ethics Monitor that may lead to a Court finding of a violation of Probation.

F. BPXP's violation of the Terms of Probation, as determined by the District Court, may constitute a breach of this Agreement. Revocation of BPXP's probation by the District Court shall constitute a material breach of this Agreement.

G. No terms of this Agreement are meant to conflict with the Terms of Probation as required by the Plea Agreement. To the extent that any requirements of this Agreement conflict with the Terms of Probation as required by the Plea Agreement, BPXP shall provide notice to the EPA Authorized Representative(s) and the EPA Independent Auditor of such conflict, and the Terms of Probation shall take precedence over and preempt the requirements of this Agreement.

2. COMPLIANCE WITH THE SEC JUDGMENT ORDER

BP p.l.c. shall comply in full with the terms and conditions of the SEC Judgment Order entered by the U.S. District Court for the Eastern District of Louisiana on December 10, 2012 in the matter of *Securities Exchange Commission v. BP p.l.c.*, 2:12-cv-2774-CJB-SS (E.D. La.). The SEC Judgment Order and all attachments or exhibits to that document are attached hereto and hereby incorporated by reference as if restated in full.

A. BP p.l.c. shall notify the EPA Authorized Representative(s) within ten (10) days of BP p.l.c.'s discovery of any violation of the terms and conditions of the SEC Judgment Order.

B. BP p.l.c. shall submit to the EPA Authorized Representative(s) and the EPA Independent Auditor any correspondence BP p.l.c. is required to submit pursuant to the SEC Judgment Order in accordance with the schedules set forth in those documents.

C. BP p.l.c.'s violation of the terms and conditions of the SEC Judgment Order, as determined by the SEC, may constitute a breach of this Agreement.

VI. COORDINATION WITH PLEA AGREEMENT MONITORS

1. BPXP shall provide the EPA Independent Auditor and the EPA Authorized Representative(s) with the reports of the Ethics Monitor and Process Safety Monitor under the Remedial Order within ten (10) days of receipt.

2. The EPA Independent Auditor shall submit all of the EPA Independent Auditor's written reports pursuant to the terms of this Agreement to the Ethics Monitor, the Third-Party Auditor (for informational purposes) and the Process Safety Monitor.

3. BPXP shall provide the Third-Party Auditor reports to the EPA Authorized Representative(s) within ten (10) days of receipt.

VII. ETHICS & COMPLIANCE

1. ETHICS & COMPLIANCE PROGRAM(S). BP p.l.c. shall continue to maintain an independent Ethics & Compliance function (not reporting to the operating businesses) to support the operating businesses and the BP Covered Entities as described in the following paragraphs.

In addition to the duties set forth under the Remedial Order, the Ethics Monitor shall have the duties set forth in this Paragraph. The Ethics Monitor shall review the programs set forth in this Section VII (Ethics & Compliance) and in paragraphs 1C, 2A and 2D of Section VIII (Corporate Governance), in accordance with the schedule set forth in the Ethics Monitor's work plan pursuant to the Remedial Order. Provided that the Ethics Monitor completes three (3) complete cycles of review during the period of this Agreement, the Ethics Monitor may exercise its discretion to make modifications to the schedule and work plans, as appropriate. The Ethics Monitor shall review, and may make recommendations for improvement with respect to, the programs set forth in the Ethics & Compliance and Corporate Governance terms identified in this paragraph and their implementation by BP p.l.c. and/or specific Group US Businesses. to the extent that such terms of this Agreement apply to BP p.l.c. and/or Group US Businesses. The Ethics Monitor may provide that certain recommendations apply only to a specific Group US Business or shall be phased in throughout Group US Businesses in an orderly manner. The Ethics Monitor shall continue to report, based on the Remedial Order review schedule, to the EPA Authorized Representative(s), the EPA Independent Auditor and BP's Authorized

Representative(s) on the status of improvements.

Upon each review, the Ethics Monitor shall prepare a written report to document the review along with any recommended or required improvements to the programs set forth in the Ethics & Compliance and Corporate Governance terms identified in this paragraph and their implementation within the applicable Group US Businesses. The report shall clearly designate which recommendations are made pursuant to the Remedial Order and which are made pursuant to this Agreement. The Ethics Monitor shall submit these reports to the EPA Authorized Representative(s), the EPA Independent Auditor and BP's Authorized Representative(s).

BPA shall cause to be implemented those final recommendations (after any dispute resolution process) resulting from the work of the Ethics Monitor under this Agreement. To the extent that BPA disputes any recommendation of the Ethics Monitor, BPA shall notify the Ethics Monitor in writing within thirty (30) days of receiving the report, and BPA and the Ethics Monitor shall meet in good faith to attempt to resolve the dispute. If the dispute cannot be resolved within forty-five (45) days after BPA provides written notice to the Ethics Monitor, BPA shall inform the EPA Authorized Representative(s) in writing, and EPA shall determine whether the recommendation shall be implemented.

2. AUDITING ETHICS & COMPLIANCE. BP p.l.c. shall conduct internal and/or commissioned external audits of Group US Businesses to be conducted with respect to key Ethics & Compliance risks each year. Audits may address one or more elements of Ethics & Compliance programs in place to meet the objectives of the BP Code of Conduct ("Code" or "Code of Conduct"), including compliance, risk assessment, internal controls or other topics. The results and/or findings of these audits shall be provided to the Group Ethics & Compliance Officer ("GE&CO"), the EPA Authorized Representative(s), the EPA Independent Auditor, the Ethics Monitor and the BP Authorized Representative(s) within ten (10) days of issuance, along with any recommendations and timelines for improvement or necessary remedial action.

3. SCHEDULE OF AUDITS. Beginning in the last quarter of 2014 calendar year, BP p.l.c. shall provide the EPA Independent Auditor, the Ethics Monitor and the EPA Authorized Representative(s) with a schedule of all formal internal and commissioned external audits planned for Group US Businesses for the calendar year pursuant to paragraph 2 of Section VII (Ethics & Compliance). The schedule of audits shall include a description of the audit, the name and contact information of any lead external auditor and, when applicable, dates or proposed dates of the audits. BP p.l.c. may modify the schedule during the course of the year.

4. ETHICS & COMPLIANCE STAFFING. The Ethics Monitor may review and make recommendations regarding general Ethics & Compliance staffing levels and resources within the Group US Businesses.

5. BP CODE OF CONDUCT.

A. BP p.l.c. shall maintain a Code of Conduct for BP Covered Entities to:

1. Provide rules and/or guidance for compliance in areas such as Health, Safety, Security and the Environment ("HSSE"); conflicts of interest; competition; trade restrictions; export controls; money laundering; and bribery and corruption.

2. Include or reference guidance to assist Employees in making proper decisions when faced with difficult situations involving Ethics or Compliance.

3. Specify that Employees are obligated to report discovery of any violations or potential violations of the Code or legal requirements. In support of this obligation, the Code shall also outline other channels available for raising concerns, including the OpenTalk program.

4. Include a zero tolerance statement against any form of retaliation against Employees or Contractors who raise good faith concerns regarding compliance, safety and/or ethics.

B. Code of Conduct Certification

1. BPA shall continue to implement MyPlan or its equivalent system.[1] BPA shall ensure that MyPlan (or equivalent) is designed so that Group US Employees who use MyPlan (or equivalent) shall submit annual certifications of their compliance with the Code by the end of the first quarter of the following calendar year. At a minimum, beginning in calendar year 2015, the Code of Conduct certification shall state that the Group US Employee has in the prior calendar year: adhered to the Code of Conduct; reported compliance concerns or exceptions through available reporting channels; and been advised about, or was aware of, the OpenTalk program. The system shall be designed so that:

   a. Beginning with certifications for the calendar year 2014, Group US Employees who use MyPlan (or equivalent) shall be required to certify annually through MyPlan that they are familiar with the Code of Conduct and have complied with the Code, except for breaches that he or she has reported.

   b. Group US Employees using MyPlan (or equivalent) who are hired on or after July 1, 2014 shall certify, no later than the first completed cycle of MyPlan that they have read the Code and agree to abide by it.

[1] MyPlan is a performance evaluation system generally used by Group US Employees, components of which include certifications and performance priorities. Certifications for calendar year 2013 were completed in early 2014. The calendar year 2014 cycle will be completed in early 2015.

2. Beginning with certifications for calendar year 2014, BPA shall require Group US Business and function Senior Level Leaders who use MyPlan (or equivalent) and who have direct reports who are Group US Employees to certify as part of the review under MyPlan (or equivalent) that they have discussed with their teams as part of the My Plan review:

   a. The content and application of the Code.

   b. Encouragement to report potential Code violations and other Ethics & Compliance concerns through OpenTalk and other reporting programs.

   c. Instructions on the use of OpenTalk and other reporting programs.

   d. That BPA may take disciplinary action, including discharge, for any violation of law, regulation or the Code of Conduct.

   e. An explanation of the non-retaliation policy or statement.

C. Enforcement

1. BP Covered Entities shall continue to apply sanctions for Employees found to have breached the Code. Such sanctions may include: oral or written warnings; loss of variable compensation; dismissal and referral to appropriate authorities for civil or criminal proceedings; or other appropriate actions, depending on the nature of the breach.

2. BPA shall provide the Ethics Monitor with relevant information and documentation regarding BP p.l.c.'s development and implementation of its prior and now inactive tracking system for Code breaches within six (6) months of the Effective Date of this Agreement.

3. BP Covered Entities shall continue to impose consequences as appropriate, including but not limited to those sanctions set forth in paragraph 5(C)(1) of Section VII (Ethics & Compliance), herein, on Contractors working for BP Covered Entities whose performance violates the Code.

6. RISK-BASED COMPLIANCE STANDARDS AND PROCEDURES. BPA shall maintain policies and/or standards and control processes designed to prevent, detect and remediate unethical or illegal conduct with respect to Group US Businesses.

A. BPA shall continue to maintain a centrally organized, online register to record potential conflicts of interest.

B. BPA shall continue to maintain a centrally organized "gifts and entertainment" register to record receiving and giving of gifts and entertainment between Group US Employees and third parties.

7. COMMUNICATIONS REGARDING ETHICS & COMPLIANCE ISSUES. BPA shall maintain a communications plan for Group US Businesses that promotes awareness of Ethics & Compliance topics and includes: communication activities to be undertaken; the status of such activities; the channel of communications; and the timing of such messaging and actions. More specifically:

A. Communications channels and media shall be tailored to the target audience and may include, among other communications: communications in the form of posters, banners, brochures, leaflets and cards; "town hall" briefings; videos; and postings on the intranet and bp.com.

B. BP p.l.c.'s intranet shall contain an Ethics & Compliance site, which shall contain Ethics & Compliance information. Ethics & Compliance information may include, among other information: relevant Ethics & Compliance staff information; information about the OpenTalk (or equivalent) reporting channel; information on key risks faced by BP Group Entities; the Code of Conduct; links to key standards, policies and guidance; and summaries of certain OpenTalk cases and actions taken based upon these cases.

C. The BP Group Chief Executive ("GCE") shall continue to set the tone from the top by annually communicating to all Employees with respect to expectations regarding compliance with the Code of Conduct.

8. ETHICS & COMPLIANCE TRAINING. As set forth in this paragraph, Ethics & Compliance Training shall include Code of Conduct training, targeted Ethics & Compliance training and ethical leadership training.

A. Code of Conduct Training for Employees

1. Beginning in the last quarter of calendar year 2014, and on an annual basis thereafter, BPA shall provide Ethics & Compliance training that includes one (1) or more topics under the Code of Conduct to Group US Employees, and BP Affiliates with Foreign Business shall provide Ethics & Compliance training that includes one (1) or more topics under the Code of Conduct to their Employees. The first annual training shall be completed no later than March 1, 2015.

2. BPA shall provide training on the Code of Conduct for all new Group US Employees hired on or after July 1, 2014, and BP Affiliates with Foreign Business shall provide a training program on the Code of Conduct for all of their new Employees hired on or after January 1, 2015. The training

program shall be designed to provide training for each new Employee no later than ninety (90) days after their date of hire.

3. The Code of Conduct training program for Group US Employees and Employees of BP Affiliates with Foreign Business shall:

   a. Reference and reinforce the availability of the OpenTalk system.

   b. Emphasize the importance of compliance with laws and regulations requiring reporting of financial and other information to government agencies.

   c. Emphasize the importance of adherence to operating, safety and process standards in maintaining a safe workplace.

   d. Emphasize the importance of ethical conduct and adherence to the Code of Conduct.

B. Targeted Compliance Training for Group US Employees

1. Beginning in the last quarter of 2014 calendar year, BPA shall annually identify appropriate positions occupied by Group US Employees for targeted compliance training and the subject matter of the training, and shall prepare a plan for providing such targeted compliance training. Targeted compliance training shall cover one (1) or more Ethics & Compliance topics, such as: Our Code; Anti-Bribery and Corruption; Anti-Money Laundering, Competition and Anti-Trust; Trade Sanctions; and Conflicts of Interest. New Group US Employees hired into those positions identified for targeted training shall receive this training within one (1) year of hire.

C. Leadership Training Program for Senior Level Leaders

1. BPA shall continue to provide leadership training for BP Senior Level Leaders and above who are Group US Employees, and BP Affiliates with Foreign Business shall provide leadership training for BP Senior Level Leaders who are their Employees.

2. BP Senior Level Leaders and above subject to paragraph 8(C)(1) of Section VII (Ethics & Compliance) who are hired or promoted into such positions on or after July 1, 2014 shall receive leadership training within the first year of hire or promotion into such positions.

3. The leadership training program required by paragraph 8(C)(1) of Section VII (Ethics & Compliance) currently includes the following objectives:

a. Define ethics and articulate the business case for ethical behavior.

b. Describe the impact that personal values have on behavior and decision making.

c. Describe effective ethical decisions using a structured decision making model.

d. Identify leadership behaviors necessary to create and sustain an ethical culture.

e. Identify leadership behaviors necessary to create and sustain a speaking up culture.

f. Encourage ethical leadership.

9. TRACKING OF TRAINING

A. BPA shall continue to develop a centralized database to track, among other things, Ethics & Compliance training provided to Group US Employees, subject to review by the Ethics Monitor.

B. Upon full implementation of the centralized database, BPA shall maintain the database to track the completion of Code of Conduct, targeted compliance and leadership training sessions by Group US Employees.

C. BPA shall retain relevant documentation (such as summaries and training materials) used in the course of such training for the duration of this Agreement.

10. REPORTING AVENUES

A. OpenTalk. BP p.l.c. shall maintain the OpenTalk program as permitted by law in the applicable jurisdiction, or a substantially similar replacement program, that allows Employees, Contractors or any other third party to raise concerns or seek guidance about Ethics & Compliance or the Code of Conduct.

1. BPA shall post the dedicated contact information for OpenTalk at the usual place for posting employment-related information and on the company's intranet site.

2. The OpenTalk program shall continue to provide Employees and Contractors access twenty-four (24) hours a day, seven (7) days a week. Concerned individuals shall be able to contact OpenTalk through a number of avenues such as the web, fax, telephone or letter, and shall be able to maintain their anonymity (unless legally impermissible in their jurisdiction).

3. BPA shall continue to promote awareness of OpenTalk. Any such program to promote awareness shall include signage or other forms of communications directed at Employees without computer access. The program shall provide information about speaking up, listening, and taking actions consistent with the obligations under the Code of Conduct.

4. On an annual basis, and consistent with applicable privacy laws, the GE&CO shall compile a summary report of information pertaining to the nature, status and outcome of significant investigations resulting from calls to OpenTalk originating in the applicable BP Covered Entities during the previous year, and provide that report to the EPA Authorized Representative(s), the Ethics Monitor and the EPA Independent Auditor.

5. During the term of the Agreement, BPA shall maintain a system for tracking concerns reported to OpenTalk related to Group US Businesses.

11. NON-RETALIATION STATEMENT. BP Covered Entities shall prohibit retaliation, reprisal or harassment by any Employees against any individual, including an Employee, Contractor, Contract Personnel or consultant for making any report or notification raising any good faith questions or concerns related to issues regarding: an actual or potential violation(s) of this Agreement; an actual or potential violation of any federal, state or local law or regulation; or an actual or potential violation of the Code of Conduct or other rules or policies. BP Covered Entities shall take appropriate action, in accordance with the BP Code of Conduct, against any Employee who violates the non-retaliation statement.

12. FRAUD AND MISCONDUCT INVESTIGATIONS. In accordance with BP p.l.c's Fraud and Misconduct Reporting Standard and its Investigation Guidelines, as they may be amended or revised from time to time:

A. BPA shall review reportable allegations of fraud and misconduct related to the applicable Group US Businesses that are reported to Ethics & Compliance, the Fraud and Misconduct Investigation Team or other recognized channels for reporting. BPA shall investigate credible allegations, and the results of these investigations shall be recorded.

B. Results from investigations conducted under subparagraph 12(A) above involving findings of fraud or misconduct, and any proposed corrective actions, shall be reviewed by the appropriate leader in the applicable Group US Business where the incident occurred. That leader shall be responsible for implementing corrective actions, within the applicable Group US Business.

13. EMBEDDING COMPLIANCE PROGRAMS AT THE BUSINESS UNIT LEVEL. BPA shall continue to embed Ethics & Compliance Leaders ("ECLs") in Group US Businesses. The ECLs shall support and assist in the implementation of Ethics & Compliance standards, training and communications in their respective Group US Businesses.

A. Current ECL job responsibilities include:

1. Encouraging Group US Employees and Contractors who work for Group US Businesses to speak up about Ethics & Compliance issues, including through the use of OpenTalk;

2. Supporting or facilitating, as appropriate, the delivery of Ethics & Compliance training, including Code of Conduct training;

3. Meeting or communicating with management teams for their respective Group US Businesses and with the respective Ethics & Compliance Regional Directors on matters related to Ethics & Compliance;

4. Maintaining awareness of the overall Ethics & Compliance risks that have been identified for the particular business in which the ECL is located, and recommending interventions as needed;

5. Communicating broader Ethics & Compliance issues to the Ethics & Compliance function; and

6. Staying informed of Ethics & Compliance issues through regular communications and contact between ECLs and Ethics & Compliance staff associated with their respective business.

B. The job responsibilities set forth above may be amended from time to time provided that ECLs continue to support and assist in the implementation of Ethics & Compliance standards, training and communications in their respective Group US Businesses.

14. INCENTIVES FOR INDIVIDUALS AND BUSINESS UNITS.

A. BP p.l.c. or BPA shall maintain an Employee compensation system for Group US Businesses which includes a variable pay plan, or annual cash bonus, paid to eligible (non-union) Group US Employees on an annual basis. The variable pay plan will continue to provide variable pay contingent upon both individual and business unit performance using key objectives, including key safety goals and metrics.

B. BP p.l.c. or BPA shall maintain the MyPlan evaluation system, or a similar replacement system, for eligible Group US Employees. The MyPlan evaluation system, or similar replacement system, shall require all eligible Group US Employees to work with their supervisors to set objectives for job performance in the following areas, among others: (1) contributions to safety, compliance and risk management, which includes compliance with the Code of Conduct, laws and regulations; (2) values and behaviors; and (3) personal development actions.

Under this system, eligible Group US Employees shall be required to submit annual certifications of their compliance with the Code of Conduct, which shall continue to require compliance with all applicable regulations.

C. The compensation of Group US Businesses' Executive Leaders at Level D or above shall continue to be explicitly tied to safety performance and operational risk management through BP p.l.c.'s "Group Performance Factor" or a similar replacement mechanism. Bonus stock awards for such executives shall continue to be dependent on meeting criteria which include an assessment of safety and environmental sustainability (*i.e.*, reinforcement of safety culture within BP).

15. AWARD/SPOT BONUS INCENTIVE PROGRAM. BPA shall maintain an award program by which managers in Group US Businesses may reward Group US Employees with cash bonuses and/or other recognition for outstanding contributions to the company's ethical culture, compliance with HSSE principles and regulatory compliance assurance. BPA shall provide awards to selected Group US Employees.

16. KAPLAN REPORT REVIEW AND IMPLEMENTATION. BPA shall provide the Kaplan Report (an evaluation of BP p.l.c.'s Ethics & Compliance programs by an outside consultant) to the EPA Independent Auditor, the EPA Authorized Representative(s) and the Ethics Monitor. The Ethics Monitor shall consider all recommendations in the Kaplan Report and may incorporate Kaplan Report recommendations in its reviews, as appropriate.

17. ETHICS MONITOR REVIEW OF SYSTEMIC ISSUES. The Ethics Monitor shall be provided an opportunity to review past culture assessments and surveys, including any employee engagement surveys (including methodology and implementation) conducted for Group US Businesses for a period of not greater than five (5) years prior to the Effective Date of this Agreement. Additionally, using the methodology identified in his Work Plan at Section II.B., the Ethics Monitor shall review the existing culture and compliance environment at Group US Businesses. The Ethics Monitor will provide his findings and conclusions as part of his reports to the BP Authorized Representative(s), the EPA Authorized Representative(s) and the EPA Independent Monitor.

VIII. CORPORATE GOVERNANCE

1. EXECUTIVE AND BOARD OVERSIGHT OF ETHICS & COMPLIANCE FUNCTION

A. BP p.l.c. Board of Directors. The BP p.l.c. Board of Directors ("BP p.l.c. Board") and its committees shall, consistent with applicable law, provide oversight regarding BP Covered Entities' performance under this Agreement. Such oversight shall comprise compliance with the matters described in the remainder of this sub-paragraph A (publication of Board governance principles), the following sub-paragraph B (maintenance of MBAC and SEEAC committees or replacement committees), considering reports from the GE & CO as described in paragraph 2B of this Section VIII, and paragraphs 3 and 4 of this Section VIII

(Board Recognition and Annual Reporting). The BP p.l.c. Board shall continue to maintain documented "Board Governance Principles" and shall continue to make the documentation available on the BP public website. Any change to the "Board Governance Principles" shall be documented and made available on the BP public website.

B. The BP p.l.c. Board shall maintain the Safety, Ethics and Environmental Assurance Committee ("SEEAC") and the Main Board Audit Committee ("MBAC") (or replacement committees) that are accountable for their oversight functions as set forth in the "Board Governance Principles." The SEEAC and MBAC currently are accountable for the following oversight functions:

1. With respect to SEEAC:

   a. Monitoring and obtaining assurance that the GCE's internal control system for operations is designed and implemented effectively in support of his observance of the relevant executive limitations.

   b. Monitoring and obtaining assurance that the management or mitigation of significant BP risks of a non-financial nature is appropriately addressed by the GCE.

   c. Receiving and reviewing regular reports from the GCE, or his delegate, the Group Internal Auditor and the GE&CO regarding the GCE's adherence to the relevant executive limitations and his management in responding to risk.

   d. Reviewing material to be placed before shareholders which addresses environmental, safety and ethical performance and making recommendations to the BP p.l.c. Board about their adoption and publication.

   e. Reviewing reports on the BP Group Entities' compliance with the Code of Conduct and on its employee concerns program, OpenTalk (or its equivalent replacement system), as it relates to non-financial issues.

   f. Recommending to the BP p.l.c. Board any changes or further delineation of the executive limitations in relation to non-financial matters.

2. With respect to MBAC:

   a. Monitoring and obtaining assurance that the GCE's internal control system is designed and implemented effectively in support of his observance of the relevant executive limitations.

b. Monitoring and obtaining assurance that the management or mitigation of significant BP risks of a financial nature is appropriately addressed by the GCE.

c. Receiving and reviewing regular reports from the GCE, or his delegate, the Group Internal Auditor and the GE&CO regarding the GCE's adherence to the relevant executive limitations and his management in responding to risk.

d. Monitoring and obtaining assurance that the legally required standards of disclosure are being observed.

e. Reviewing financial disclosure documents to be placed before shareholders or filed with regulatory bodies and making recommendations to the BP p.l.c. Board about their adoption and publication.

f. Monitoring and reviewing the effectiveness of BP's internal audit function.

g. Reviewing BP's internal financial controls and its systems of internal control and risk management.

h. Reviewing and monitoring the external financial auditor's independence, objectivity and the effectiveness of the audit process and recommending to the BP p.l.c. Board the appointment, reappointment and removal of the external auditor and approving the auditor's remuneration and terms of engagement.

i. Implementing and monitoring policy on the engagement of the external auditor to supply non-audit services to BP.

j. Reviewing the systems in place, including OpenTalk (or equivalent replacement system), enabling those who work for BP Group Entities to raise, in confidence, any concerns about possible improprieties in matters of financial reporting or other financial issues and for those matters to be appropriately investigated.

k. Recommending to the BP p.l.c. Board any changes or further delineation of executive limitations in relation to financial matters.

C. BP p.l.c. shall continue to maintain the Ethics & Compliance Committee ("ECC"), or a similar replacement executive committee, subject to any changes required or recommended by the Ethics Monitor. The ECC shall continue to: provide oversight and direction to BP's Ethics & Compliance program; meet on a

quarterly basis; and be chaired by the GCE and/or the GE&CO. The ECC shall continue to be responsible for:

1. Reviewing further development of the Ethics & Compliance program, including new initiatives and improvements, and monitoring Ethics & Compliance performance, including training, audits and certifications;

2. Reviewing significant Ethics & Compliance risks that are identified by Ethics & Compliance and the plans that are in place to manage those risks; and

3. Reviewing and endorsing Ethics & Compliance standards on behalf of BP's executive-level leadership and disseminating the standards as appropriate.

D. BPA Board Oversight. The BPA Board of Directors (the "BPA Board") shall, consistent with applicable law, provide oversight regarding BPA's performance under this Agreement.

2. REPORTS FROM THE GE&CO. The GE&CO shall:

A. Report directly to BP p.l.c.'s General Counsel at least once per quarter on matters involving the BP Group Entities' Ethics & Compliance and the Ethics & Compliance requirements of this Agreement. BP p.l.c. shall maintain a record of: (a) the occurrence of meetings between the GE&CO and the BP p.l.c. General Counsel pertaining to this Agreement; and (b) the fact that Ethics & Compliance and the requirements of this Agreement were discussed.

B. Have direct access, and annually report orally and in writing, to the BP p.l.c. Board of Directors' committees, SEEAC and MBAC, on matters relating to BP p.l.c.'s Ethics & Compliance, and the Ethics & Compliance requirements of this Agreement and their implementation. BP p.l.c. shall maintain a record of: (a) the occurrence of such reports; and (b) the fact that Ethics & Compliance and the requirements of this Agreement and their implementation were discussed.

C. Meet at least annually with the BPA Board to report orally and in writing on matters relating to Ethics & Compliance, and the Ethics & Compliance requirements of this Agreement and their implementation. BPA shall maintain a record of: (a) the occurrence of such meetings; and (b) the fact that the Ethics & Compliance requirements of this Agreement and their implementation were discussed.

D. Meet at least annually with BP p.l.c.'s Executive Team to report orally and in writing on matters relating to the BP Group Entities' Ethics & Compliance and the Ethics & Compliance requirements of this Agreement and their implementation. BP p.l.c. shall maintain a record of: (a) the occurrence of such

meetings; and (b) the fact that the Ethics & Compliance requirements of this Agreement and their implementation were discussed.

3. BOARD RECOGNITION. Respondents shall furnish this Agreement to all members of their respective Boards of Directors at their next regularly scheduled meetings after May 1, 2014. Each of the Respondents also shall furnish a written summary and oral presentation of this Agreement to all members of their Boards of Directors at the next regularly scheduled meetings of those Boards after May 1, 2014. For the duration of this Agreement, each of the Respondents shall provide new members to their Boards with a written summary or copy of this Agreement no later than ninety (90) days from their appointment to a Board. Each of the Respondents shall maintain records reflecting that the actions required pursuant to this paragraph have been taken.

4. ANNUAL REPORTING TO THE BOARDS. BP p.l.c. shall provide a copy of each annual report prepared pursuant to Section X (BP Covered Entities' Annual Reports) of this Agreement to the Boards of Directors of each of the Respondents. Each of the Respondents shall maintain records reflecting its respective Boards' consideration of these annual reports as well as their respective Boards' decisions or directions to management, if any, in response to information in the reports.

5. MAINTAINANCE OF GE&CO POSITION. BP p.l.c. shall maintain the position of GE&CO (or equivalent) dedicated to the BP Group Entities' overall Ethics and Compliance and charged with fulfilling the duties of the GE&CO as set forth in this Agreement. The current GE&CO is Maryann Clifford. BP p.l.c. shall notify the Ethics Monitor, the EPA Independent Auditor and the EPA Authorized Representative(s) of any change in the GE&CO position and shall provide a copy of the resume of the new GE&CO no later than ten (10) days after selection. BP p.l.c. shall consult with the Ethics Monitor with respect to the appropriate qualifications and skills of a new GE&CO prior to making that selection.

IX. PROCESS SAFETY

1. APPLICABILITY OF OCSLA. BPXP, BPXA and any Affiliates participating in activities in the waters of the U.S. (collectively, "BPXP/BPXA Entities") are subject to the requirements of the Outer Continental Shelf Lands Act, 43 U.S.C. § 1331 *et seq.*, ("OCSLA") and its implementing regulations to the extent set forth therein. For purposes of this Agreement, "waters of the U.S." shall have the same definition as in the Implementation Plan. (*See* Implementation Plan, Section B (Definitions), Paragraph 17.)

2. BSEE REGULATORY COMPLIANCE AND CRITERIA FOR UNACCEPTABLE PEFORMANCE. This Agreement shall not supersede or replace the BPXP/BPXA Entities' ongoing legal obligations to comply with OCSLA and the Department of the Interior Bureau of Safety and Environmental Enforcement ("BSEE") regulations at 30 C.F.R. Parts 203-291. If, in accordance with 30 C.F.R. § 250.135, after providing notice and an opportunity for review, BSEE determines that a BPXP/BPXA Entity's operating performance is unacceptable, and BSEE refers such determination of unacceptable performance to the Bureau of Ocean Energy Management ("BOEM"), EPA may consider the unacceptable performance to be a material

breach of this Agreement. BSEE shall promptly notify the EPA Authorized Representative(s) if it refers a determination of unacceptable performance by a BPXP/BPXA Entity to BOEM pursuant to 30 C.F.R. § 250.135-.136. BSEE and BOEM reserve the right to take any other action they deem appropriate to address or respond to a BPXP/BPXA Entity's unacceptable operator performance, in accordance with their statutory and regulatory authority. Such BSEE or BOEM action shall be independent of any review or process undertaken or determination made by EPA under this Agreement.

3. CONTRACTOR OVERSIGHT. With respect to deepwater drilling operations (*see* Implementation Plan, Section B (Definitions), Paragraph 8) in waters of the U.S., the BPXP/BPXA Entities shall maintain:

A. Contract Governance Boards for review and approval of deepwater drilling rig contracts and cementing contracts for deepwater drilling operations;

B. Contractor audits and correction of Contractor safety management deficiencies prior to hiring or using a new deepwater drilling rig Contractors and new cementing Contractors in deepwater drilling operations;

C. Maintenance of a list of approved deepwater drilling rig Contractors and cementing Contractors for deepwater drilling activities; and

D. A process to address areas for Contractor performance improvement with respect to process safety management for deepwater drilling rig Contractors and cementing Contractors retained for deepwater drilling operations to the extent such areas are identified in the course of Contractor performance management reviews or other means adopted by the BPXP/BPXA Entities.

4. SEMS REQUIREMENTS. For any offshore facility that is subject to BSEE's Safety and Environmental Management System ("SEMS") regulations at 30 C.F.R. §§ 250.1900-1933, the BPXP/BPXA Entities shall:

A. Within thirty (30) days of the Effective Date of this Agreement, provide the EPA Authorized Representative(s) with the SEMS audit schedule for the remainder of the calendar year, and provide an updated schedule annually thereafter;

B. No later than thirty (30) days following BSEE approval of the SEMS audit plan, provide the EPA Authorized Representative(s) with the BSEE-approved SEMS audit plan for the facility being audited; and

C. No later than thirty (30) days following the completion of each SEMS audit, provide an audit report of the findings to the EPA Authorized Representative(s), including deficiencies identified and a Corrective Action Plan ("CAP") for addressing the deficiencies.

Failure to provide a SEMS audit schedule, audit plan, audit report or CAP, and/or failure to timely and fully comply with the CAP with respect to deficiencies may be considered by EPA to be a material breach of this Agreement.

5. SEMS AUDIT REPORTING TO PROCESS SAFETY MONITOR. By no later than thirty (30) days following the completion of each SEMS audit, BPXP shall provide the Process Safety Monitor with the audit plan, a comprehensive report of all audit findings, not limited to identified regulatory deficiencies, but including all areas of concern and opportunities for improvement identified by the SEMS auditor, in order to assist the Process Safety Monitor in fulfilling his or her duties under the Remedial Order. BPXP shall facilitate access for the Process Safety Monitor to each SEMS lead auditor at the conclusion of each SEMS audit if the Process Safety Monitor requests a discussion of the findings and recommendations of a given audit and/or a description of how the audit was conducted in order to fulfill his or her duties under the Remedial Order.

6. PROCESS SAFETY MONITOR.

A. Within thirty (30) days after the DOJ and BPXP comment period under the Remedial Order, BPXP shall provide a copy of the Remedial Order work plan to the EPA Authorized Representative(s) and BSEE for work to be performed by the Process Safety Monitor appointed under the Remedial Order.

B. Within ten (10) days following issuance, BPXP shall provide the EPA Authorized Representative(s) with the Process Safety Monitor's written reports containing the initial and follow up reviews and recommendations in accordance with the Remedial Order.

C. Consistent with the process and requirements set forth in the Remedial Order, BPXP shall adopt the recommendations of the Process Safety Monitor. Failure to adopt the recommendations pursuant to the process and requirements of the Remedial Order shall constitute a material breach of this Agreement.

D. BPXP shall ensure that resources, including funding and personnel, are made available for BPXP to implement the recommendations of the Process Safety Monitor, as required under the Remedial Order. Failure to adequately fund and provide personnel for implementation of those recommendations shall constitute a material breach of this Agreement.

7. TRACKING LEADING AND LAGGING INDICATORS. Within ninety (90) days of the Effective Date of this Agreement, BPXP shall begin tracking and reporting a range of leading and lagging indicators for personnel and process safety consisting of: losses of primary containment; reported injury frequency; number of reportable incidents; and overdue SEMS CAP items and such other indicators as BPXP and BSEE may agree to in writing. These safety metrics shall be: reported to the BPXP Board of Directors; provided in the BP Covered Entities' annual report; and provided to BSEE.

8. GLOBAL WELLS ORGANIZATION. BP p.l.c. shall maintain a Global Wells Organization ("GWO") or similar entity that provides deepwater drilling expertise. The GWO shall continue to maintain its own Safety and Operational Risk Committee, or similar committee.

9. GULF OF MEXICO COMPLIANCE MANAGEMENT SYSTEM. BPXP shall establish and maintain a Gulf of Mexico compliance management system, or similar system to track regulatory requirements. BPXP shall continue to periodically update the compliance management system to reflect new requirements promulgated by BSEE and other agencies, as necessary.

10. BLY REPORT. BPXP shall: (a) provide to the EPA Authorized Representative(s), the Process Safety Monitor and the Ethics Monitor the Bly Report and recommendations; and (b) make available to the EPA Authorized Representative(s) and Process Safety Monitor, as requested, the reports of the current independent expert or similar entity or individual retained by the BP p.l.c. Board to assess progress on implementation of the Bly Report recommendations. The Process Safety Monitor may consider all recommendations in the Bly Report and any of the expert's findings in its review, as appropriate.

X. BP COVERED ENTITIES' ANNUAL REPORTS

1. ANNUAL REPORT. On or before March 31, 2015 and annually thereafter, BP Covered Entities shall prepare and submit a consolidated written report to the EPA Authorized Representative(s), the Ethics Monitor, the Third-Party Auditor (for informational purposes) and the EPA Independent Auditor describing the measures taken by the applicable BP Covered Entities during the previous calendar year to ensure compliance with this Agreement ("Annual Report"). The final report shall be submitted no earlier than sixty (60), and no later than thirty (30), days prior to the end of this Agreement.

These Annual Reports shall include, but not be limited to, the following items pursuant to the terms of this Agreement.

A. Information required to summarize the applicable BP Covered Entities' activities pursuant to Sections V through XII of this Agreement. For purposes of this Agreement, documentation evidencing compliance with Sections V through XII of this Agreement shall also be made available to the EPA Independent Auditor and the EPA Authorized Representative(s) as an accompaniment to the Annual Report.

B. The status of any legal proceedings for which reporting is required under paragraph 5 of Section XII (General Provisions) of this Agreement. The status shall include the initiation, times, places and subject matter of search warrants, subpoenas, criminal charges or criminal or civil agreements identified in paragraph 5 of Section XII.

C. A summary report identifying: the date, responsible business unit and general type or classification of all OpenTalk reports from Group US Businesses; the number

of reports in each general type or classification; and information regarding any corrective actions related to significant reports made to the OpenTalk program.

D. A report summarizing the information required by paragraph 7 of Section XII (General Provisions) of this Agreement.

E. A summary of any findings made by the EPA Independent Auditor under this Agreement during the previous review cycle, and any unresolved findings from the EPA Independent Auditor from prior review cycles and the status of corrective measures being implemented with respect to such recommendations.

F. The certifications required by paragraph 3 of Section XII (General Provisions) of this Agreement.

G. A list of all current BP Covered Entities, and their classification (*e.g.*, BP Affiliate with Foreign Business, Respondent, etc.).

H. Information on leading and lagging indicators required by paragraph 7 of Section IX (Process Safety) of this Agreement.

2. ADDITIONAL SUBMISSION TO ETHICS MONITOR. For purposes of identifying adequate corporate governance responses, upon submission of the annual report, the Group US Businesses shall separately submit to the Ethics Monitor a consolidated summary report by the Fraud and Misconduct Committee and the Fraud and Misconduct Investigation Team (or their equivalents) providing metrics related to allegations of fraud and misconduct brought to the attention of the Fraud and Misconduct Committee and the Fraud and Misconduct Investigation Team during the preceding calendar year with respect to Group US Businesses. Such submission shall track each matter with a unique identification number, describe the nature of the matter (e.g. retaliation, etc.), the approximate date of the incident, the business unit or operation in which the matter occurred, the status of the matter, and the final resolution of the matter and provide summary metrics on the information in the report. Matters pending resolution at the time of a reporting period shall be reported to the Ethics Monitor in the next annual submission until final resolution of the matter is reported.

XI. EPA INDEPENDENT AUDITOR

1. SELECTION OF THE EPA INDEPENDENT AUDITOR. BPA shall engage, at its own expense and without recourse to EPA, an experienced Independent Auditor whose qualifications are acceptable to the EPA to serve as the EPA Independent Auditor for the oversight of this Agreement.

A. Within ninety (90) days after the Effective Date of this Agreement, BPA shall provide the EPA Suspension and Debarment Director ("EPA SDD Director") with a list of at least two (2) proposed EPA Independent Auditors for EPA's approval. BPA's submission should contain the name, telephone number, email address,

current position, resume and duties of each of the potential EPA Independent Auditors. BPA shall also provide a statement by the proposed EPA Independent Auditors on its ability to access the appropriate resources to effectively audit this Agreement and its past experience with managing resources to audit similar Agreements.

B. Should the EPA SDD Director determine that none of BPA's proposed EPA Independent Auditors are acceptable for the purposes of this Agreement, BPA shall promptly nominate additional proposed EPA Independent Auditors for approval by EPA within thirty (30) days of notification of denial.

C. Upon notification by EPA that the SDD Director has determined that any one (1) or all of the proposed EPA Independent Auditors are acceptable, BPA shall select one (1) of the EPA Independent Auditors whose qualifications were acceptable to the EPA SDD Director to serve as the EPA Independent Auditor for this Agreement.

D. BPA shall enter into a contract with the EPA Independent Auditor for the performance of duties in this Agreement within sixty (60) days of notification that a nominee is acceptable to the EPA SDD Director. The EPA-approved EPA Independent Auditor selected by BPA shall provide an agreed upon work plan to be performed by the EPA Independent Auditor, in accordance with the scope and provisions of this Agreement, as soon as possible, but no later than sixty (60) days after the EPA Independent Auditor has entered into a contract.

E. Any change of the EPA Independent Auditor requires prior approval from EPA. Should EPA become concerned with the performance of the EPA Independent Auditor, the EPA Authorized Representative(s) will raise those concerns to the BP Authorized Representative(s) and the EPA Independent Auditor. If EPA's concerns are not resolved promptly, the EPA Authorized Representative(s) shall refer the matter to the EPA Suspension and Debarment Counsel, who in consultation with the EPA SDO, may require BPA to propose a new EPA Independent Auditor within sixty (60) days of EPA's notification. BPA agrees to propose and hire a new EPA Independent Auditor upon notification from EPA. The same process and time requirements for the initial selection of the EPA Independent Auditor as set forth in this provision apply for selection of a replacement EPA Independent Auditor.

F. It is BPA's responsibility to hire a qualified auditor. Due to general standards of ethical conduct for government employees, no EPA official or employee may direct BPA to hire a particular individual or firm as an EPA Independent Auditor. BPA will not request that any representative of EPA identify or suggest qualified monitors.

2. NATURE AND GENERAL TERMS OF EMPLOYMENT

A. Nature of Employment. The EPA Independent Auditor serves to provide an independent verification of the applicable BP Covered Entities' compliance with this Agreement. The EPA Independent Auditor shall not be an agent of the BP Group Entities, and his or her work shall not be subject to the BP Group Entities' assertion of the attorney-client or work product privilege doctrines. The EPA Independent Auditor shall be an independent party who is appropriately certified, licensed or otherwise adequately qualified, and who has had no previous business relationship with BP Covered Entities in the five (5) years prior to the Effective Date of this Agreement that would create an actual or perceived conflict of interest in monitoring the applicable BP Covered Entities' compliance with this Agreement. Notwithstanding the foregoing, the Third-Party Auditor, Process Safety Monitor, and Ethics Monitor appointed by DOJ under the Remedial Order may be eligible to be considered as an EPA Independent Auditor candidate under this Agreement.

B. Annual Certification of Independence. Upon nomination, and upon each anniversary of the Effective Date of this Agreement, BPA shall furnish EPA with an affidavit from the EPA Independent Auditor certifying that he or she has no financial, professional, personal, familial or other interest that would create an actual or apparent conflict of interest with the BP Covered Entities or the BP Covered Entities' Employees, other than that arising from the appointment as the EPA Independent Auditor or as the Third-Party Auditor under the Remedial Order. The affidavit must also certify that his or her representation of any other client will not create an actual or apparent conflict of interest in fulfilling his or her responsibilities as EPA Independent Auditor.

C. Confidentiality. The EPA Independent Auditor shall maintain as confidential all non-public information, documents and records it receives from BP Covered Entities, subject to the EPA Independent Auditor's reporting requirements herein and paragraph 8 of Section XII (General Provisions). The EPA Independent Auditor shall take appropriate steps to ensure that any of his or her consultants or employees shall also maintain the confidentiality of all such non-public information.

3. SCOPE OF INDEPENDENT AUDITOR'S COMPLIANCE DUTIES

A. Particular Duties. The EPA Independent Auditor shall:

1. Conduct an annual review of applicable BP Covered Entities' compliance with Sections V through XII of this Agreement and draft a report summarizing each such review.

2. Receive and review the reports and other information required to be provided to the EPA Independent Auditor under Section VI of this Agreement.

3. Review BPA's annual compliance certification with this Agreement and Annual Reports.

4. Submit its findings in an annual written report to the BP Authorized Representative(s), the Ethics Monitor, the Process Safety Monitor (for informational purposes) and the EPA Authorized Representative(s) within ninety (90) days after each anniversary of the Effective Date of this Agreement. The final annual report shall be submitted to the BP Authorized Representative(s), the Ethics Monitor and the EPA Authorized Representative(s) no earlier than sixty (60), and no later than thirty (30), days prior to the termination of the Agreement.

5. If the EPA Independent Auditor identifies a potential violation of law or regulation as an incidental consequence of auditing compliance with this Agreement, and if the EPA Independent Auditor deems it appropriate, the EPA Independent Auditor shall inform the relevant BP Covered Entity and/or the EPA Authorized Representative(s).

6. If either (a) BPA's certification or report identifies a deficiency in compliance, or (b) the EPA Independent Auditor identifies a deficiency in compliance, the EPA Independent Auditor shall so report to the EPA Authorized Representative(s) and the BP Authorized Representative(s), and the relevant BP Covered Entity shall develop a timely and appropriate corrective action plan for the identified non-compliance, the implementation of which the EPA Independent Auditor shall review as part of its compliance assessment.

B. Scope of Annual Compliance Assessment. The EPA Independent Auditor shall verify the applicable BP Covered Entities' compliance with Sections V through XII of this Agreement as follows:

1. It is the expectation of the parties that the EPA Independent Auditor's annual compliance review can be completed based on: (a) the BP Covered Entities' Annual Reports under this Agreement, and supporting documentation as outlined in Section X (BP Covered Entities' Annual Reports); (b) BP Covered Entities' annual certifications; (c) reports and records provided by the Ethics Monitor and the Process Safety Monitor; (d) interviews with the Ethics Monitor and Process Safety Monitor; and (e) District Court findings with respect to the Plea Agreement or the SEC Judgment Order. In the event that the EPA Independent Auditor determines that it is unable to verify compliance on that basis, the EPA Independent Auditor shall be provided the same access to records,

documents and other information as the EPA Authorized Representative(s) as set forth in paragraph 8 of Section XII (General Provisions) of this Agreement, subject to the specific provisions and limitations in subparagraphs 2 through 5, below.

2. With respect to Section V (Compliance With Other Agreements), Section VI (Coordination with Plea Agreement Monitors) and paragraphs 6C and 6D of Section IX (Process Safety) of this Agreement, and the status of any recommendations of the Ethics Monitor or Process Safety Monitor, the EPA Independent Auditor's annual compliance reviews shall be completed based on the BP Covered Entities' annual reports under this Agreement, any reports or other submissions under the Remedial Order of the Ethics Monitor or Process Safety Monitor, interviews with the Process Safety Monitor or Ethics Monitor as the EPA Independent Auditor deems appropriate and any findings of the U.S. District Court with respect to BPXP's probation and the SEC Judgment Order.

3. With respect to Section VIII (Corporate Governance) of this Agreement, requests by the EPA Independent Auditor for additional information from the relevant BP Covered Entities' Boards shall be directed to and completed by the BP Authorized Representative(s) by providing further documentation of compliance to the EPA Independent Auditor.

4. With respect to the Ethics & Compliance training in paragraph 8 of Section VII (Ethics & Compliance) of this Agreement, the EPA Independent Auditor's first annual compliance review shall address BPXP; the second annual compliance review shall address Group US Businesses; and annual compliance reviews thereafter shall address BP Covered Entities.

5. As set forth in paragraph 8 of Section XII (General Provisions) of this Agreement, EPA may at its discretion conduct audits of the applicable BP Covered Entities' compliance with the terms of this Agreement. EPA may elect to have the EPA Independent Auditor accompany and assist EPA on the audit at the BP Covered Entities' expense. The EPA Independent Auditor, at EPA's election, may conduct audit activities set forth in paragraph 8 of Section XII (General Provisions) of this Agreement, including but not limited to: interviewing the applicable BP Covered Entities' Employees; reviewing the applicable BP Covered Entities' files or other records required pursuant to this Agreement; touring the applicable BP Covered Entities' facilities; developing documents to prepare for the interview; and drafting the Audit Report.

XII. GENERAL PROVISIONS

1. LANGUAGES. All communications to Group US Employees, including but not limited to written materials, oral communication and training required under this Agreement, will be provided in English or, if the Group US Employee has a limited ability to read, write, speak or understand English, in another language in which the Group US Employee is sufficiently fluent so that each Employee can understand the communication.

2. NOTICE TO EMPLOYEES AND SENIOR LEVEL LEADERS. BPA will notify Group US Employees, and BP p.l.c. will notify Employees of BP Affiliates with Foreign Business, within sixty (60) days of the Effective Date of this Agreement, of: the fact and substance of this Agreement; the facts related to the Plea Agreement; and the importance of each such Employee abiding by the terms and conditions of this Agreement and the Code of Conduct. BPA may provide the required notification to Group US Employees by posting the Agreement on BP p.l.c.'s intranet site and sending an email or other similar communication to Employees notifying them of such posting. BP p.l.c. shall supplement the intranet posting in another appropriate manner for Employees of BP Affiliates with Foreign Business, such as email communication, town hall meetings, targeted posting of notices or new Employee training.

3. CORPORATE OFFICIAL'S CERTIFICATION. As part of the Annual Reports required by Section X (BP Covered Entities' Annual Reports) of this Agreement, the BP p.l.c. GE&CO and/or the relevant Corporate Secretary of each Respondent shall certify that applicable Respondent is in compliance with its respective obligations under paragraphs 1, 3 and 4 of Section VIII (Corporate Governance) of this Agreement. The certification shall state:

> I certify under penalty of law that, [except as set forth below], based on my reasonable inquiry of the persons within the applicable Respondent who manage the applicable Respondent's obligations under the Administrative Agreement and of my review of information generated during the course of the applicable Respondent's performance under this Agreement, to the best of my knowledge, the applicable Respondent is in compliance with its respective obligations under Paragraphs 1, 3, and 4 of the Administrative Agreement.

If the Respondent's designated officer cannot so certify with respect to any particular obligation, term or condition, the certification shall identify the deficiency and the corrective measures being taken or to be taken to achieve compliance.

The BP Covered Entities agree that nothing in this paragraph shall limit the EPA SDO's ability to take an action pursuant to paragraph 19 of Section XII (General Provisions) of this Agreement (Breach of Agreement/Survival of Cause for Debarment).

4. TRUTHFULNESS IN REPORTING AND CONVEYING INFORMATION TO EPA AND OTHER REGULATORY AGENCIES. The BP Covered Entities shall comply with their obligations under federal law or regulation to provide accurate information to EPA or its designees and to other Federal Government Entities, including the Department of the Interior. Within sixty (60) days of the Effective Date of this Agreement, BP Covered Entities shall

provide written notification to the BP Covered Entities' Principals of the commitment to cooperate fully with all requests for information and inquiries from the EPA SDO, the EPA Suspension and Debarment Division, the Ethics Monitor and the EPA Independent Auditor made pursuant to this Agreement.

5. REPORTS OF LEGAL PROCEEDINGS. Except as set forth in Attachment 30, and with the exception of the ongoing civil litigation, administrative proceedings and investigation involving the *Deepwater Horizon* blowout, explosion and spill, BP Covered Entities represent that, to the best of their knowledge, no BP Covered Entities: (a) have been informed that they are currently the target or subject of an ongoing U.S. federal criminal investigation; or (b) are currently named in an action of the kind set forth in paragraphs (A) through (D), below.

Beginning on July 1, 2014, Respondents shall notify the EPA Authorized Representative(s) on or before the beginning of each calendar quarter of any of the following matters:

A. The initiation of any criminal investigation or civil enforcement action by any Federal Government Entity involving allegations of any violation(s) of federal environmental laws, the Foreign Corrupt Practices Act, false statements, false claims, kickbacks, conflict of interest or antitrust laws, if Respondents have been informed that they or any BP Covered Entity or Principal of a BP Covered Entity is a target or subject of such investigation. In the case of a Principal, such allegations must be related to duties performed by the Principal in the course of employment. For the purposes of this paragraph, "initiation" in a criminal investigation shall mean the issuance of a subpoena, the execution of a search warrant, or the filing of formal charges; "initiation" in a civil enforcement action shall mean the filing of a judicial or administrative complaint (but not the issuance of a notice of violation or incident of noncompliance), the service of administrative subpoenas (but not information requests or inspections) or the issuance of show cause orders.

B. Initiation of qui tam actions or citizen action suits against a BP Covered Entity or any of their Principals by any person or entity alleging: violations of any U.S. federal environmental laws or the Foreign Corrupt Practices Act; false statements to Federal Government authorities or in public filings, including filings required by U.S. securities laws; false claims for government reimbursement, kickbacks, conflict of interest; or anti-trust violations. For purposes of this paragraph, the term "citizen action suit" shall mean a private enforcement action expressly authorized by a U.S. statute.

C. Criminal charges or suspension or debarment actions brought by any Federal Government Entity against a BP Covered Entity or any of their Principals in a matter relating to the business of the BP Covered Entity.

D. Any conviction or guilty plea, *nolo contendere* plea, deferred prosecution agreement, pre-trial diversion agreement, civil judgment or civil judicial consent

decree in a matter brought by a Federal Government Entity to which any BP Covered Entities are parties in a matter relating to the business of the BP Covered Entity.

E. Nothing in this paragraph shall be interpreted to require any BP Covered Entity to disclose information that is subject to the attorney-client privilege, work product doctrine or other applicable legal privilege.

6. ELECTRONIC TRACKING OF FORMAL ENFORCEMENT ACTIONS. BPA shall develop, implement and maintain a database or computerized system for tracking those matters identified in paragraph 5 of Section XII (General Provisions) of this Agreement.

7. REPORTS OF MISCONDUCT. During the term of this Agreement, BP Covered Entities shall timely disclose in writing to the EPA Authorized Representative(s), the Ethics Monitor and the EPA Independent Auditor whenever, in connection with the award, performance or closeout of a federal procurement or nonprocurement covered transaction, any BP Covered Entity or Principal of a BP Covered Entity has credible evidence that BP Covered Entity's Employee has committed: (a) a violation of Federal criminal law involving fraud, conflict of interest, bribery or gratuity violations found in Title 18 of the U.S. Code; or (b) a violation of the civil False Claims Act, 31 U.S.C. §§ 3729-3733.

BP Covered Entities will investigate all credible reports of such misconduct that come to their attention and will notify the EPA Authorized Representative(s), the Ethics Monitor and the EPA Independent Auditor of the outcome of such investigations and any potential or actual impact on any aspect of BP Covered Entities business with a Federal Government Entity. The BP Covered Entity will take corrective action, including prompt restitution when established by a court or a tribunal with competent jurisdiction or agreed upon between the parties, of any harm to the Federal Government. BP Covered Entities will include summary reports of the status of each such investigation to the EPA Authorized Representative(s) in the reports submitted pursuant to this Agreement until each matter is finally resolved. This requirement does not in any way waive BP Covered Entities' obligations to submit reports pursuant to any other section in this Agreement or to the requirements of Federal Acquisition Regulation ("FAR") 9.406-2 (b)(1)(vi) and 9.407-2 (a)(8), if applicable, or any other statutory or regulatory reporting requirement.

Nothing in this paragraph shall be interpreted to require BP Covered Entities to disclose information that is subject to the attorney-client privilege, work product doctrine or other applicable legal privilege.

8. GOVERNMENT AUDITS AND ACCESS TO RECORDS AND INFORMATION. In addition to any other right the Federal Government may have by statute, regulation or contract, the EPA Authorized Representative(s) may, for the purpose of verifying BP Covered Entities' compliance with the terms and conditions of this Agreement, evaluate each of BP Covered Entities' books, records and other company documents and supporting materials (collectively, "BP Covered Entities' Records") including:

A. BP Covered Entities' business conduct in its dealings with all of its customers, including the Federal Government;

B. BP Covered Entities' compliance with federal laws, regulations and procurement policies; and

C. BP Covered Entities' compliance with the requirements of Federal Government contracts, leases, covered transactions or subcontracts,

The materials described above, except to the extent that such documents are subject to attorney-client privilege, work product or other applicable legal privilege, shall be made available by BP Covered Entities at all reasonable times for inspection or audit. The EPA Authorized Representative(s) may evaluate reports, records or other documents of the EPA Independent Auditor, the Ethics Monitor, the Process Safety Monitor and the Third-Party Auditor. Further, if EPA determines that an annual report of the EPA Independent Auditor is not sufficient for the purposes of evaluating the BP Covered Entities' compliance with this Agreement and, after notice and consultation, the BP Covered Entities are unable to resolve the concern, EPA may enlist the EPA Independent Auditor in further audit activities under this provision. For purposes of this provision, the EPA Authorized Representative(s), the Ethics Monitor or the EPA Independent Auditor may interview any Group US Employee at the Employee's place of business during normal business hours, or at such other place and time as may be mutually agreed between the Employee and the EPA Authorized Representative(s), the Ethics Monitor or the EPA Independent Auditor. Group US Employees may be interviewed without a representative of the BP Group Entities' Employees or Principals being present. The Group US Employee may be represented personally by his or her own counsel or other representative, if requested by the Employee. The Employee also may decline to be interviewed.

Respondents agree to pay to the U.S. Treasury as miscellaneous receipts the reasonable costs actually incurred by EPA personnel or its authorized agents for conducting such records examinations during the term of this Agreement. The parties agree that "cost" shall include reasonable expenses for travel, transportation, lodging and meals, to the extent normally authorized under federal rules governing Federal Government travel, as such expenses are actually incurred by EPA personnel or its authorized agents in conducting site visits for the purpose of verifying compliance with this Agreement. No part of the payments for costs in accordance with this provision shall be an allowable cost under any EPA or Federal Government contract, subcontract or nonprocurement covered transaction.

As an alternative to an onsite audit of BP Covered Entities' compliance with the terms and conditions of this Agreement, EPA may, at its sole election, conduct an audit by mail in which instance BP Covered Entities shall provide documentation of their compliance with this Agreement, including but not limited to copies of documentation maintained as required in this Agreement and such additional documentation and/or certifications as may be requested by EPA.

9. SALE OF THE RESPONDENTS' BUSINESSES. The sale, assignment, or transfer of ownership of BP Covered Entities' business or any divisions, subsidiaries, Affiliates, business units, facilities, offices or other corporate components (collectively "assets") shall not be

executed as an artifice to avoid being subject to the Agreement. However, this Agreement is not intended to restrict the lawful and legitimate sale, assignment, or transfer of ownership of assets through an arm's length transaction and would not bind an asset purchaser who purchases through an arm's length transaction.

With respect to the sale, assignment or transfer of more than fifty percent (50%) of a Respondent's assets to an unaffiliated entity pursuant to an arm's length transaction, including but not limited to the transfer of operational control of a jointly owned asset to an unaffiliated third party, such third party shall not be liable for the BP Covered Entities' obligations and the BP Covered Entity shall remain obligated to comply with the terms and conditions of this Agreement with respect to all non-disposed assets but not with respect to the sold, assigned or transferred assets or assets for which operational control has been transferred. The Respondent shall send notification to the EPA Authorized Representative(s) and the EPA Independent Auditor no less than thirty (30) days after the date of sale. The notification shall be signed and dated, and shall state in writing: the date of the sale; the name(s), address(es) and contact person(s) representing the purchaser(s) on the sale; a specific description of subject business or property being sold; and certify in writing whether said sale is an arm's length transaction.

In the event that any Respondent sells or in any way transfers ownership of any BP Covered Entity in its entirety to a third party, the BP Covered Entity shall send notification to the EPA Authorized Representative(s) and the EPA Independent Auditor no less than thirty (30) days prior to the closing date of the sale. The notification shall be signed and dated, and shall state in writing: the date of the planned sale; the name(s), address(es) and contact person(s) representing the purchaser(s) on the sale; a specific description of subject business or property being sold; and certify in writing whether said sale is an arm's length transaction.

10. BP GROUP ENTITIES' PURCHASE OF BUSINESSES. In the event that any BP Group Entity purchases or establishes new business units in the U.S. or new BP Affiliates With Foreign Business during this Agreement, such BP Group Entity shall implement provisions of this Agreement, as applicable, including any training or education requirements, within one hundred eighty (180) days following such purchase or establishment. Should the BP Group Entity be unable to integrate such purchase or establishment within one hundred eighty (180) days, the BP Group Entity shall notify the EPA Authorized Representative(s) in writing, and shall provide a timeline for complete integration, which will be subject to EPA approval. The BP Group Entity shall be notified of EPA's decision on the integration plan within thirty (30) days of receipt. If the EPA Authorized Representative(s) does not respond within sixty (60) days of receipt, the BP Group Entity's proposed timeline shall be deemed approved.

If, during the period covered by this Agreement, a BP Group Entity acquires or gains control (other than through a joint venture) of any business concern, which enters into procurement or covered non-procurement transactions with the U.S., the EPA Authorized Representative(s) shall be notified within thirty (30) days after the closing of the transaction. Such notice shall state the name, address, nature of the business concern and any work it has done for any Government Entities over the last year.

11. RESTRUCTURING OR ACQUISITION OF NEW BUSINESSES. BP Group Entities shall not, through a change of name; business reorganization, restructuring or realignment; sale or purchase of assets; or similar action, seek to avoid the obligations and conditions set forth in this Agreement.

12. HIRING INELIGIBLE INDIVIDUALS. Beginning thirty (30) days after the Effective Date of this Agreement, prior to any Principal becoming employed in a US Respondent's business, US Respondents shall make reasonable inquiry into the status of that potential employee which shall include a review of the System for Award Management ("SAM") as maintained by the General Services Administration ("GSA") on the internet (https://www.sam.gov) for federal procurement and nonprocurement programs. The results from all SAM searches shall be kept in Respondent's records.

13. INELIGIBLE EMPLOYEES. BP Covered Entities are not required to terminate the employment of individuals who are or become suspended, debarred, proposed for debarment or otherwise ineligible as prescribed by any Federal Government Entity debarment program during their employment with BP Covered Entity. However, the BP Covered Entity will remove such Employees from responsibility for, or involvement with, business affairs related in any manner whatsoever with Federal Government covered procurement or non-procurement transactions or programs until the final resolution of such suspension or proposed debarment.

If any BP Covered Entity is aware that its Employee is debarred, the BP Covered Entity shall notify the EPA Authorized Representative(s) of such debarment and the reasons therefore, and of whatever personnel action has been taken or will be taken against the Employee, within thirty (30) days of the BP Covered Entity's knowledge of the debarment.

If any BP Covered Entity learns that any Principal is charged with a U.S. federal criminal offense relating to business activities or otherwise relating to honesty or integrity, the BP Covered Entity will remove that Principal immediately from responsibility for, or involvement with, business affairs as related in any manner to Federal Government procurement or covered nonprocurement transactions.

14. BUSINESS RELATIONSHIPS WITH SUSPENDED OR DEBARRED ENTITIES. For the purposes of specifically fulfilling their obligations under Federal procurement or nonprocurement covered transactions, BP Covered Entities shall not knowingly form a contract with, purchase from, or enter into any procurement or covered nonprocurement transaction (as defined at 48 C.F.R. Subpart 9.4, and 2 C.F.R. Part 180 and relevant agency implementing rules) with any individual or business entity that is listed on SAM as debarred, suspended, proposed for debarment or otherwise ineligible at the time of such procurement or nonprocurement award or transaction.

BP Covered Entities may enter into a business relationship or continue a federally funded procurement or nonprocurement covered transaction with a suspended or debarred Contractor/participant if: (a) the BP Covered Entity submits to EPA in writing the compelling reasons that justify entering into a business transaction with a person listed on SAM as soon as possible, but not later than sixty (60) days prior to entering into such a business relationship; and

(b) the EPA SDO approves the request to enter into the transaction. EPA shall respond to the request within thirty (30) days of receipt of the request. Unless otherwise indicated in writing by EPA, each request must be made on a transaction by transaction basis. The BP Covered Entity shall keep documentation of all search results and certifications that are required pursuant to this provision.

15. FUTURE MISCONDUCT DURING AGREEMENT. In matters unrelated to the matters addressed herein, EPA may find that a BP Covered Entity has materially breached this Agreement based on any misconduct that occurs during the period of the Agreement that may lead to any action taken pursuant to 2 C.F.R. § 180.700 or 2 C.F.R. § 180.800.

16. RESPONDENTS' LEGAL OBLIGATIONS. Nothing in this Agreement shall be deemed to limit a BP Covered Entity's obligations under any federal, state or local law or regulation, nor does this Agreement limit in any manner EPA's ability to enforce any law or regulation within EPA's jurisdiction.

17. UNALLOWABLE COSTS. BP Covered Entities agree that all costs, as defined in FAR 31.205-47, incurred by, for, or on behalf of any BP Covered Entity or any current or former officer, director, agent, Employee, consultant or Affiliate of BP Covered Entities shall be expressly unallowable costs for Federal Government contract or covered transaction accounting purposes. Unallowable costs include, but are not limited to, costs arising from, related to, or in connection with:

a. The matters at issue herein;

b. The Federal Government's criminal and civil investigations regarding the matters at issue herein; and

c. EPA's review of BP's present responsibility, including but not limited to the costs of the company's submissions, presentations and appearances before the EPA SDO's Office and/or the EPA SDD.

The BP Covered Entity's costs of performing and administering the terms and conditions of this Agreement, the cost of the EPA Authorized Representative(s) and any fines or penalties levied or to be levied in or arising out of the matter at issue here are agreed to be expressly unallowable costs. Also unallowable are the BP Covered Entity's costs of bringing the BP Covered Entity's self-governance and Ethics & Compliance programs to a level acceptable to the EPA Authorized Representative(s). The BP Covered Entities agree to account separately for such costs. BP Covered Entities' costs of maintaining, operating and improving their corporate self-governance/compliance/ethics programs that are incurred after expiration of this Agreement, may be allowable costs.

BP Covered Entities agree to treat as unallowable costs the full salary and benefits of any officer, Employee or consultant terminated from their employ or removed from Federal Government contracting as a result of the wrongdoing at issue here and the cost of any severance payments or early retirement incentive payments paid to Employees released from the BP

Covered Entity as a result of the wrongdoing at issue here. For purposes of the preceding sentence, the salary and benefits costs shall include all such costs from the first instance of participation of each individual in the matters at issue here, as determined by the EPA Authorized Representative(s).

BP Covered Entities recognize that in order to comply with the terms and conditions of this paragraph, certain costs may need to be reclassified. BP Covered Entities shall proceed immediately to identify and reclassify such costs and, within ninety (90) days of the Effective Date of this Agreement, BP Covered Entities shall adjust any bid rate, billing rate or unsettled final indirect cost rate pools to eliminate any costs made unallowable by this Agreement, and shall advise the EPA Authorized Representative(s), the cognizant administrative contracting officer and the cognizant Federal Government auditor of the amount and nature of the reclassified costs within one hundred and twenty (120) days of the date of this Agreement.

18. ADVERSE ACTIONS. Each BP Covered Entity avers that adverse actions taken, or to be taken by it against any Employee or other individual associated with any BP Covered Entity arising out of or related to the matters at issue herein were not the result of any action by, or on behalf of, agents or employees of the U.S.

19. BREACH OF AGREEMENT/SURVIVAL OF CAUSE FOR DEBARMENT. A BP Covered Entity's failure to meet any of its obligations pursuant to the terms and conditions of this Agreement, if determined by the EPA SDO to be a material breach of this Agreement by that BP Covered Entity, shall constitute a separate cause for suspension and/or debarment of that BP Covered Entity. Violation of multiple non-material provisions, or repeated violations of a non-material provision, of this Agreement by a BP Covered Entity may cumulatively constitute a material breach of the Agreement by that BP Covered Entity. The underlying causes for debarment survive the execution of this Agreement, and EPA may initiate suspension or debarment proceedings against a BP Covered Entity or statutorily disqualify a BP Covered Entity on these grounds if there is a material breach of this Agreement. Nothing in this provision or this Agreement shall be construed as a waiver of any legal rights of a BP Covered Entity to contest the EPA SDO's determination of materiality or breach.

20. RESOLUTION OF DEBARMENT, SUSPENSION, OR STATUTORY DISQUALIFICATION. Upon execution of this Agreement, EPA, as Lead Agency in this matter pursuant to the Interagency Suspension and Debarment Committee process, shall terminate the suspension of BP Covered Entities and shall lift the statutory disqualification of BPXP as well as the statutory disqualifications of BPXA based on its November 29, 2007 CWA conviction and BPPNA based on its March 12, 2009 CAA conviction. In addition, provided that the terms and conditions of this Agreement are faithfully fulfilled, EPA, as Lead Agency, will not suspend, debar, or otherwise reinstate the statutory award disqualification of, a BP Covered Entity, as applicable, based on: (i) the *Deepwater Horizon* explosion, spill and cleanup, and matters related thereto, including the January 29, 2013 *Deepwater Horizon* conviction, the December 10, 2013 SEC Judgment Order and any judgment in civil litigation in which a BP Covered Entity is a defendant; (ii) the November 29, 2007 CWA conviction of BPXA; or (iii) the March 12, 2009 CAA conviction of BPPNA. EPA's decision, which is based upon the facts at issue here, shall not restrict EPA or any other agency of the Federal Government from instituting

administrative actions, including, without limitation, suspension, debarment or statutory disqualification should:

a. Other information—indicating the propriety of such action come to the attention of EPA or such other Federal Government agency and such information provides an independent cause for suspension or debarment unrelated to the *Deepwater Horizon* explosion, spill and cleanup; or

b. Additional facts concerning the *Deepwater Horizon* explosion, spill and cleanup be discovered by the Federal Government which were not disclosed by Respondents or otherwise produced to, or in the possession of, the Federal Government, prior to the Effective Date of this Agreement, including in any litigation related to the *Deepwater Horizon* explosion, spill and cleanup, and such facts provide an independent cause for suspension or debarment.

This Agreement relates solely to suspension, debarment and statutory disqualification issues, pursuant to 48 C.F.R. Subpart 9.4 and 2 C.F.R. Part 180, and 33 U.S.C. § 1368(a), in conjunction with the circumstances recited herein and in no way waives any criminal, civil, contractual or any other administrative remedy or right which the Federal Government may have for the circumstances so described in this Agreement.

21. CONCLUSION OF DEBARMENT PROCEEDINGS. BP Covered Entities hereby waive all further notice and opportunity for hearing to which they may otherwise be entitled to but for the terms and conditions of this Agreement except that BP Covered Entities shall receive such notice(s) as they would otherwise be entitled if paragraphs 19 or 20 of Section XII (General Provisions) of this Agreement are invoked.

22. RELEASE OF LIABILITY. BP Covered Entities hereby release the U.S., its instrumentalities, agents and employees in their official and personal capacities, of any and all liability or claims arising out of or related to the November 28, 2012 suspension of Respondents and Covered Affiliates, the February 1, 2013 CWA disqualification of BPXP at its Houston headquarters, the negotiation of this Agreement, the suspension, proposed debarment, or debarment of Respondents or Covered Affiliates and the discussions leading to this Agreement and all matters related to the February 26, 2008 and March 20, 2009 statutory disqualification notices.

Within seven (7) days after the Effective Date of this Agreement, Respondents shall enter into a stipulation of dismissal with EPA pursuant to Fed. R. Civ. P. 41(a)(1)(ii), which stipulation shall provide that the August 12, 2013 Complaint filed in the U.S. District Court for the Southern District of Texas against EPA, the EPA Administrator, the EPA SDO and EPA employees in civil case number 4:13-cv-2349 is dismissed with prejudice, with each party bearing its own fees and costs.

Within fifteen (15) days after the Effective Date of this Agreement, BPXP shall withdraw with prejudice its administrative appeal of BOEM's May 31, 2013 and June 27, 2013 decision

letters pending before the Interior Board of Land Appeals (IBLA 2013-0194), each party to bear its own costs.

23. RESPONSIBILITY. This Agreement is not an endorsement of BP Group Entities' ethics and compliance, corporate governance, process safety, or other programs. The SDO is only resolving the administrative actions herein based upon the BP Covered Entities' obligations to comply with the terms of this Agreement. By entering into this Agreement, EPA does not address any finding of responsibility under 48 C.F.R. § 9.104 or other applicable federal nonprocurement regulations for any specific Federal Government procurement or nonprocurement transaction. BP Covered Entities' compliance with the terms and conditions of this Agreement may constitute a contributing factor to be considered when rendering a responsibility finding for a specific government procurement or nonprocurement transaction.

24. RESTRICTION ON USE. BP Covered Entities shall not use any term or condition of this Agreement, or the fact of the existence of this Agreement, for any purpose related to the defense of, or in mitigation of, any criminal, civil or administrative investigation, proceeding or action except as set forth below.

Notwithstanding the restriction on use herein, the existence and substance of this Agreement may be used (a) to respond to Federal Government civil or administrative demands for injunctive relief, otherwise addressed by the terms of this Agreement or (b) in any criminal, civil or administrative matter in which the other party introduces evidence of this Agreement or of the suspension, debarment or statutory disqualifications which this Agreement resolves, or (c) in any matter initiated by any Government Entity to suspend, debar, or otherwise render ineligible or find not responsible a BP Covered Entity based on the events giving rise to this Agreement and the matters addressed herein.

The use of any term or condition of this Agreement, or the fact of the existence of this Agreement shall be strictly limited to the purposes for which this Agreement is used as provided under (a), (b) or (c) of this paragraph.

25. BANKRUPTCY. A BP Covered Entity shall not use bankruptcy proceedings to affect the enforcement of this Agreement in the interests of the Federal Government.

26. ENTIRE AGREEMENT. This Agreement constitutes the entire agreement between the parties and supersedes all prior agreements and understandings, whether oral or written, relating to the subject matter hereof. This Agreement shall be binding upon and inure to the benefit of and be enforceable by the parties hereto and their respective successors and assigns.

27. COUNTERPARTS. This Agreement may be executed in one (1) or more counterparts, each of which shall be an original, but all of which taken together, shall constitute one and the same Agreement.

28. SEVERABILITY. In the event that any one or more of the provisions contained in this Agreement shall for any reason be held to be invalid, illegal or unenforceable in any respect, such invalidity, illegality or unenforceability shall not affect other provisions of this Agreement.

29. PARAGRAPH HEADINGS. The paragraph headings in this Agreement are inserted for convenient reference only and shall not affect the meaning or interpretation of this Agreement.

30. MODIFICATION. This Agreement may be amended or modified only by a written document signed by EPA and Respondents and shall become effective only upon acceptance by the EPA SDO. Respondents may request to terminate this Agreement effective as of the termination of BPXP's probation described in paragraph 1 of Section V. Any request for modification or termination by Respondents shall be submitted to the EPA Authorized Representative(s). Requests shall be denied, approved or approved as modified by the EPA SDO within thirty (30) days of the EPA Authorized Representative's(s') receipt of said request.

The Plea Agreement Ethics Monitor may also request to modify this Agreement with written authorization from Respondents. Such requests shall be submitted to the EPA Authorized Representative(s) and shall become effective only upon acceptance by the EPA SDO. Requests shall be denied, approved or approved as modified by the EPA SDO within thirty (30) days of the EPA Authorized Representative's(s') receipt of said request.

31. AUTHORIZED REPRESENTATIVES. All matters involving this Agreement shall be coordinated through the Authorized Representatives listed below, including but not limited to questions, requests and other communication. BP Covered Entities shall provide EPA thirty (30) days written notice prior to any change to the designation of Respondents' Authorized Representative(s).

To Respondents (BP Covered Entities' Authorized Representative(s)):

Gabe Cuadra
Gabriel.Cuadra@bp.com
(713) 323 3777
501 Westlake Park Blvd.
Houston, TX 77079

To EPA (EPA Authorized Representative(s)):

Peggy Anthony
anthony.peggy@epa.gov
(202) 564-5364

U.S. Postal Service:

United States Environmental Protection Agency
Office of Grants and Debarment
Suspension and Debarment Division (3902-R)
1200 Pennsylvania Avenue, NW
Washington, D.C. 20460
Attn: Peggy Anthony

Express Mail or Courier: United States Environmental Protection Agency
Office of Grants and Debarment
Suspension and Debarment Division (3902-R)
1300 Pennsylvania Avenue, NW
Washington, D.C. 20004
Attn: Peggy Anthony

or such other address as either party shall have designated by notice in writing to the other party.

32. NOTICES. Any notices, reports or information required hereunder shall be in writing and delivered or mailed by registered or certified mail, by electronic mail, or by hand delivery to the appropriate Authorized Representative(s) at the address listed in paragraph 31 of this Section.

33. PUBLIC DOCUMENT. This Agreement, including all attachments and reports submitted pursuant to this Agreement, subject to the restrictions under the Privacy Act and exemptions in accordance with the Freedom of Information Act, is a public document and may be distributed by EPA throughout the Federal Government and entered into Federal Government database systems as appropriate, and provided to other interested persons upon request. It is BP Covered Entities' responsibility to claim as Confidential Business Information ("CBI") and privileged documents and communications, per the Freedom of Information Act, any and all documents attached to and submitted pursuant to the requirements of this Agreement. If CBI is not claimed at the time such documentation is submitted to EPA, BP Covered Entities hereby agree that they have waived such claim and have no objection to EPA releasing such information to the public, as appropriate.

A copy of this Agreement will be entered into the Federal Awardee Performance and Integrity Information System and, as required by law or regulation, the fact of entry or a copy of the Agreement will be posted on any other public website.

34. EPA RELIANCE. Respondents and BP Covered Entities' signatories hereto represent that, subject to criminal penalties pursuant to 18 U.S.C. § 1001, all written materials and other information supplied to EPA by its Authorized Representative(s) during the course of discussions with EPA preceding this Agreement were true, current, accurate and complete at the time of submission, to the best of their information and belief. Respondents also represent that they have provided to EPA information in their possession relating to the facts at issue. Respondents understand that this Agreement is executed on behalf of EPA in reliance upon the truth, accuracy and completeness of all such information.

35. RECORDS RETENTION. BP Covered Entities shall maintain all records necessary or incidental to this Agreement, including but not limited to those records specifically identified by terms in this Agreement, for no less than sixty (60) months subsequent to the expiration of this Agreement.

36. MAINTENANCE OF PRIVILEGE. Nothing in this Agreement shall be interpreted to require a BP Covered Entity to disclose information that is subject to the attorney-client privilege, work product doctrine or other applicable legal privilege.

37. TIME IS OF THE ESSENCE. Time is of the essence with respect to the performance of, compliance with and receipt of the benefit of all rights, duties and obligations herein. If EPA should provide additional time for a BP Covered Entity to comply with any specific deadline hereunder, such tolerance by EPA shall not be construed as a waiver or modification for any future deadlines as required herein.

38. RESPONDENT'S SIGNATORY(IES). The signatories below are fully authorized to execute this Agreement, and each represents that he or she has authority to bind the BP Covered Entities for which he or she has signed.

39. ENDORSEMENT BY SUSPENSION AND DEBARMENT OFFICIAL. This Agreement shall become effective only upon its approval and endorsement by the EPA SDO.

40. TERM. The period of this Agreement shall be five (5) years from the date of endorsement by the EPA SDO.

XIII. PARTIES' ENDORSEMENTS

FOR BP p.l.c. AND ON BEHALF OF COVERED AFFILIATES

Rupert Bondy — 13th March 2014

NAME — DATE

TITLE Group General Counsel

FOR BPA

NAME — DATE

TITLE

FOR BPXP

NAME — DATE

TITLE

FOR BPPNA

NAME — DATE

TITLE

FOR BPXA

NAME — DATE

TITLE

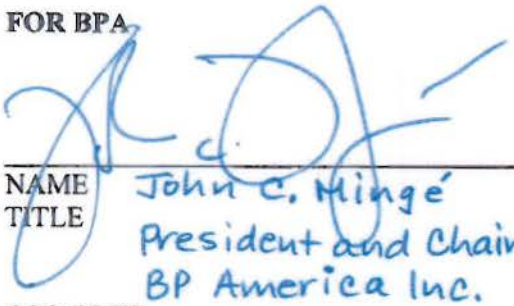
XIII. PARTIES' ENDORSEMENTS

FOR BP p.l.c. AND ON BEHALF OF COVERED AFFILIATES

_____ _____

NAME DATE
TITLE

FOR BPA



3/12/14

_____ _____

NAME John C. Minge DATE
TITLE President and Chairman
BP America Inc.

FOR BPXP

_____ _____

NAME DATE
TITLE

FOR BPPNA

_____ _____

NAME DATE
TITLE

FOR BPXA

_____ _____

NAME DATE
TITLE

XIII. PARTIES' ENDORSEMENTS

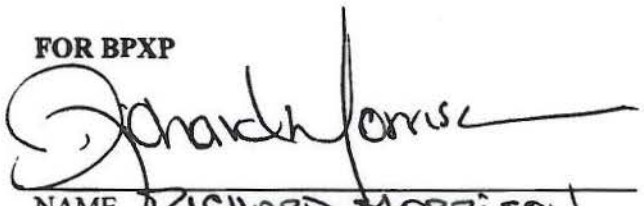
FOR BP p.l.c. AND ON BEHALF OF COVERED AFFILIATES

_____ _____
NAME DATE
TITLE

FOR BPA

_____ _____
NAME DATE
TITLE

FOR BPXP



13 MARCH 2014
NAME RICHARD MORRISON DATE
TITLE PRESIDENT, GULF OF MEXICO

FOR BPPNA

_____ _____
NAME DATE
TITLE

FOR BPXA

_____ _____
NAME DATE
TITLE

XIII. PARTIES' ENDORSEMENTS

FOR BP p.l.c. AND ON BEHALF OF COVERED AFFILIATES

_____ _____

NAME DATE
TITLE

FOR BPA

_____ _____

NAME DATE
TITLE

FOR BPXP

_____ _____

NAME DATE
TITLE

FOR BPPNA

 March 12, 2014

NAME DATE
TITLE

FOR BPXA

_____ _____

NAME DATE
TITLE

XIII. PARTIES' ENDORSEMENTS

FOR BP p.l.c. AND ON BEHALF OF COVERED AFFILIATES

_____ _____

NAME DATE
TITLE

FOR BPA

_____ _____

NAME DATE
TITLE

FOR BPXP

_____ _____

NAME DATE
TITLE

FOR BPPNA

_____ _____

NAME DATE
TITLE

FOR BPXA

Bruce Williams 3/12/2014

NAME BRUCE WILLIAMS DATE
TITLE VP. OPERATIONS

FOR THE UNITED STATES ENVIRONMENTAL PROTECTION AGENCY

NAME
Debarment Counsel
EPA Suspension and Debarment Division

3/12/14
DATE

NAME
Debarment Counsel
EPA Suspension and Debarment Division

3/12/14
DATE

NAME
Debarment Counsel
EPA Suspension and Debarment Division

3/12/14
DATE

Stephanie Ebright

NAME
Debarment Counsel
EPA Suspension and Debarment Division

3/12/14
DATE

COORDINATING AGENCY CONCURRENCE

FOR THE UNITED STATES DEPARTMENT OF THE INTERIOR

Debra E. Sonderman
Director
Office of Acquisition and Property Management

MAR 12 2014
DATE

SUSPENSION AND DEBARMENT OFFICIAL'S ENDORSEMENT

Having reviewed the terms and conditions of the above Administrative Agreement between the U.S. Environmental Protection Agency and BP Covered Entities, and in reliance on the representations, covenants, and terms herein, I hereby approve the said terms and conditions as an appropriate resolution of this matter. This approval is conditioned upon full compliance with all the terms and conditions of this Agreement. Any material breach or failure to comply with all the terms and conditions of this Agreement may result in a discretionary suspension or debarment or statutory disqualification as appropriate.

MAR 1 3 2014

Laura Fernandez
Acting EPA Suspension and Debarment Official

DATE

Agility Defense & Government Services, Inc.
v.
United States

No. CV-11-S-4111-NE

(N.D. Ala. June 26, 2012)

FILED
2012 Jun-26 AM 11:27
U.S. DISTRICT COURT
N.D. OF ALABAMA

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ALABAMA
NORTHEASTERN DIVISION

AGILITY DEFENSE AND GOVERNMENT SERVICES, INC., *et al.*,	)	
Plaintiffs,	)	
vs.	)	**Civil Action No. CV-11-S-4111-NE**
UNITED STATES DEPARTMENT OF DEFENSE, *et al.*,	)	
Defendants.	)	

MEMORANDUM OPINION AND ORDER

Plaintiffs, Agility Defense and Government Services, Inc., and Agility International, Inc., commenced this action against the United States Department of Defense, Secretary of Defense Leon E. Panetta, the Defense Logistics Agency, and the Director of the Defense Logistics Agency, Vice Admiral Mark D. Harnitchek, seeking declaratory and injunctive relief to lift plaintiffs' suspension from government contracting.[1] Plaintiffs moved for summary judgment, and defendants filed a cross-motion for summary judgment.[2] Upon consideration of the motions, briefs, and evidentiary submissions, the court has determined that summary judgment is due to

[1] Doc. no. 1 (Complaint).

[2] Doc. no. 6 (Plaintiffs' Motion for Summary Judgment); doc. no. 9 (Defendants' Motion for Summary Judgment).

be granted in favor of plaintiffs and against defendants.

I. LEGAL STANDARD

Federal Rule of Civil Procedure 56 provides that summary judgment "should be rendered if the pleadings, the discovery and disclosure materials on file, and any affidavits show that there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(c).[3] In other words, summary judgment is proper "after adequate time for discovery and upon motion, against a party who fails to make a showing sufficient to establish the existence of an element essential to that party's case, and on which that party will bear the burden of proof at trial." *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986). "A genuine issue of material fact 'exists only if sufficient evidence is presented favoring the nonmoving party for a jury to return a verdict for that party.'" *Farley v. Nationwide Mut. Ins. Co.*, 197 F.3d 1322, 1336 (11th Cir. 1999) (quoting *Stewart v. Happy Herman's Cheshire Bridge, Inc.*, 117 F.3d 1278, 1284-85 (11th Cir. 1997)).

"In making this determination, the court must review all evidence and make all reasonable inferences in favor of the party opposing summary judgment." *Chapman*

[3] Rule 56 was amended, effective December 1, 2010, in conjunction with a general overhaul of the Federal Rules of Civil Procedure. The Advisory Committee was careful to note, however, that the changes "will not affect continuing development of the decisional law construing and applying these phrases." Adv. Comm. Notes to Fed. R. Civ. P. 56 (2010 Amends.). Consequently, cases interpreting the previous version of Rule 56 are equally applicable to the revised version.

v. AI Transport, 229 F.3d 1012, 1023 (11th Cir. 2000) (*en banc*) (quoting *Haves v. City of Miami*, 52 F.3d 918, 921 (11th Cir. 1995)). "[A]n inference is not reasonable if it is only a guess or a possibility, for such an inference is not based on the evidence, but is pure conjecture and speculation." *Daniels v. Twin Oaks Nursing Home*, 692 F.2d 1321, 1324 (11th Cir. 1983). Moreover,

> [t]he mere existence of some factual dispute will not defeat summary judgment unless that factual dispute is material to an issue affecting the outcome of the case. The relevant rules of substantive law dictate the materiality of a disputed fact. A genuine issue of material fact does not exist unless there is sufficient evidence favoring the nonmoving party for a reasonable jury to return a verdict in its favor.

Chapman, 229 F.3d at 1023 (quoting *Haves*, 52 F.3d at 921); s*ee also Anderson v. Liberty Lobby*, *Inc.*, 477 U.S. 242, 251-52 (1986) (asking "whether the evidence presents a sufficient disagreement to require submission to a jury or whether it is so one-sided that one party must prevail as a matter of law").

When presented cross motions for summary judgment, "[t]he court must rule on each party's motion on an individual and separate basis, determining, for each side, whether a judgment may be entered in accordance with the Rule 56 standard." 10A Wright, Miller & Kane, *Federal Practice and Procedure: Civil 3d* § 2720, at 335-36 (1998) (footnote omitted). As another court within this Circuit has observed:

> "Cross motions for summary judgment do not change the standard." *Latin Am. Music Co. v. Archdiocese of San Juan of the Roman Catholic & Apostolic Church*, 499 F.3d 32, 38 (1st Cir. 2007). "'Cross

> motions for summary judgment are to be treated separately; the denial of one does not require the grant of another.'" *Christian Heritage Acad. v. Okla. Secondary Sch. Activities Ass'n*, 483 F.3d 1025, 1030 (10th Cir. 2007) (quoting *Buell Cabinet Co. v. Sudduth*, 608 F.2d 431, 433 (10th Cir. 1979)). "Even where the parties file cross motions pursuant to Rule 56, summary judgment is inappropriate if disputes remain as to material facts." *Id.*; *accord Monumental Paving & Excavating, Inc. v. Pa. Mfrs.' Ass'n Ins. Co.*, 176 F.3d 794, 797 (4th Cir. 1999) ("When considering motions from both parties for summary judgment, the court applies the same standard of review and so may not resolve genuine issues of material fact. Instead, [the court must] consider and rule upon each party's motion separately and determine whether summary judgment is appropriate as to each under the Rule 56 standard.") (citations omitted).

Ernie Haire Ford, Inc. v. Universal Underwriters Insurance Co., 541 F. Supp. 2d 1295, 1297-98 (M.D. Fla. 2008). *See also American Bankers Ins. Group v. United States*, 408 F.3d 1328, 1331 (11th Cir. 2005) ("This court reviews the district court's disposition of cross-motions for summary judgment de novo, applying the same legal standards used by the district court, viewing the evidence and all factual inferences therefrom in the light most favorable to the non-movant, and resolving all reasonable doubts about the facts in favor of the non-moving party.").

II. BACKGROUND

The facts in this case are not in dispute. Plaintiffs, Agility Defense and Government Services, Inc., and Agility International, Inc., are companies that have historically derived a significant portion of their operating revenue from contracts with the United States government. The genesis of this action lies in plaintiffs'

corporate relationship to Public Warehousing Company, K.S.C. ("PWC"), a Kuwaiti corporation that specializes in logistics. PWC owns scores of subsidiary entities. Some of those companies are direct subsidiaries of PWC, and others are indirect subsidiaries, owned by the direct subsidiaries. Plaintiff Agility Defense and Government Services, Inc. ("DGS") is a Delaware corporation with its principal place of business in Madison County, Alabama, and an indirect subsidiary of PWC.[4] There are three layers of subsidiaries between PWC and DGS.[5] Plaintiff Agility International, Inc. ("Agility") is a Delaware corporation with its principal place of business in Alexandria, Virginia, and a direct subsidiary of DGS; therefore, it also is an indirect subsidiary of PWC.[6]

The Defense Logistics Agency ("the Agency"), is a "combat support agency" of the Department of Defense. 10 U.S.C. § 193(f)(3). As its name suggests, the Agency is tasked with providing logistical support to the military and naval forces of the United States. Its Director is defendant Vice Admiral Mark D. Harnitchek.[7]

A. Suspension of Government Contractors

---

[4] *See* doc. no. 1-1 (Organizational Chart).

[5] *Id.* PWC directly owns Agility DGS Logistics Service Company, another Kuwaiti entity. That company, in turn, owns PWC Logistics Services Holding, a Dutch company. The Dutch company owns Agility DGS Holdings, Inc., an entity incorporated in an unspecified U.S. state. That holding company directly owns plaintiff DGS. *Id.*

[6] *See id.*

[7] Doc. no. 5 (Answer) ¶ 8.

The regulations controlling government contracting are found in the Federal Acquisitions Regulation System, Title 48 of the Code of Federal Regulations. The regulations empower the "suspending official" of a government agency to prevent certain contractors from doing business with the government. If a determination that a contractor has engaged in certain prohibited activity is made, the suspending official can "debar" that contractor doing business with the government for a fixed period of time, lasting up to three years. *See* 48 C.F.R. §§ 9.406-1-5. The suspending official also has the power to suspend a company or individual from government contracting pending determination of whether debarment is appropriate. *See id.* §§ 9.407-1-5. A suspension can last up to eighteen months without any formal action being taken against the suspended contractor. *See id.* § 9.407-4(b). However, once proceedings are initiated, the suspension can remain in effect until a final determination is made. *Id.*

While suspended, a contractor is placed on the "Excluded Parties List." *See* 48 C.F.R. § 9.404. Those on the Excluded Parties List are ineligible for any new government contracts.[8] Although a suspension may be issued by a single government

[8] *See, e.g.*, doc. no. 11 (Certified Administrative Record) at Bates 485 (PWC Suspension Letter) (stating that contracts will not be solicited from or awarded to the suspended company).

The administrative record in this case contains scores of documents and hundreds of pages. The court will cite to the record by providing a name or description for the document cited, as well as the "Bates" numbers stamped at the top and bottom of each page, rather than the internal pagination used in each document.

agency, it prohibits all departments of the executive branch of the federal government from doing business with the suspended entity. *Id.* § 9.407-1(d). Existing contracts generally are unaffected by suspension, and continue uninterrupted.[9] The government may award new contracts to suspended contractors if "compelling reasons justify[] continued business dealings," *Id.*: *e.g.*, the contractor is the lone supplier of a vital commodity.

B. Suspension of Plaintiffs

In November of 2009, a grand jury in the Northern District of Georgia issued an indictment alleging that PWC defrauded the federal government of over $6 Billion dollars in relation to contracts to supply food to American military personnel stationed in the Middle East.[10] As a result of that indictment, M. Susan Chadick, the suspending official at the Agency, suspended the government contracting privileges of PWC on November 16, 2009.[11] Concurrent with that suspension, Chadick also suspended three PWC subsidiaries, including plaintiff DGS.[12] During the following weeks, numerous other PWC subsidiaries were suspended, including plaintiff Agility on November 23,

---

[9] *Cf.* PWC Suspension Letter, at Bates 485 (stating that "existing contracts will not be renewed").

[10] *See* Certified Administrative Record, at Bates 403-62 (Indictment).

[11] PWC Suspension Letter.

[12] Certified Administrative Record, at Bates 481 (DGS Suspension Letter). At the time of suspension, plaintiff DGS was known as "Taos Industries, Inc." *See, e.g.*, doc. no. 1 ¶ 13.

2009.[13] The subsidiaries, including plaintiffs, were not accused of any involvement in the wrongdoing for which PWC was indicted; rather the sole basis for their suspension was their status as affiliates of PWC.[14]

1. Plaintiffs' response to suspension

As permitted by the regulations, plaintiffs submitted written responses in opposition to their suspensions.[15] In those submissions, plaintiffs argued that the suspensions were improper because they were not implicated in the indictment, which accused only PWC of wrongdoing.[16] Moreover, they noted the extensive company policies in place to prevent fraud and other improprieties in government contracting.[17]

Plaintiffs also argued that suspension was particularly inappropriate as to DGS, because of a "Special Security Agreement" ("SSA") regarding certain DGS contracts.[18] An SSA is necessary whenever a contractor working with classified or other sensitive information has foreign ownership.[19] The SSA prohibits PWC from

---

[13] Certified Administrative Record, at Bates 735 (Agility Suspension Letter).

[14] *See, e.g.*, *id.* (stating that plaintiff Agility was "suspended based on its affiliation to PWC, a criminally indicted company").

[15] Certified Administrative Record, at Bates 592-622 (Joint Response to Notices of Suspension); *id.* at Bates 783-99 (Supplemental Response of Plaintiff DGS).

[16] Joint Response to Notices of Suspensions, at Bates 595.

[17] *Id.* at Bates 606-17.

[18] *See generally* Supplemental Response of Plaintiff DGS.

[19] *See id.* at Bates 788 ("[A]n SSA is a standard mitigation measure required by the [Defense Security Service] when it determines that such an agreement is necessary to enable the Federal Government to protect against the unauthorized disclosure of information related to national security.") (bracketed alterations supplied).

exercising control over DGS, limiting its participation to deliberations and decisions of the DGS board of directors, and allowing PWC to control only a minority of those directors.[20] DGS applies the terms of its SSA to all government contracts, including those that do not involve sensitive information.[21] Thus, plaintiffs argued, the SSA prevented PWC from controlling the contracting activities of DGS.

The Agency rejected plaintiffs' arguments in response to their suspensions on December 10, 2009.[22] It noted that the compliance policies trumpeted by plaintiffs were identical to the policy that PWC had in effect, yet that company allegedly engaged in extensive fraud.[23] Additionally, the Agency stated that the terms of the SSA made it clear that PWC had day-to-day interaction with DGS, undermining any argument that the SSA guaranteed the independence of DGS from PWC.[24] The Agency found that "protection of the Government's interests requires the continued exclusion [of plaintiffs] from contracting with the U.S. Government."[25]

2. Litigation in Washington, D.C.

---

[20] *Id.* at Bates 788-89.

[21] *Id.* at Bates 789 ("In view of this broad language in the SSA, the exclusions of PWC's involvement extend beyond classified controls to encompass the operation of [DGS's] business affairs in general.") (bracketed alteration supplied).

[22] Certified Administrative Record, at Bates 1269-78 (Memorandum of Decision on the Request for Termination of Suspensions).

[23] *Id.* at Bates 1273.

[24] *Id.* at Bates 1275.

[25] *Id.* at Bates 1278 (bracketed alteration supplied).

Concurrently with the submission of their responses to the Agency, plaintiffs filed suit in the United States District Court for the District of Columbia, seeking injunctive relief to prevent the suspension from taking effect. Judge Richard W. Roberts held a November 23, 2009 hearing on plaintiffs' motion for a temporary restraining order, and denied that motion by oral order on December 11, 2009.[26] The suspension went into effect, and plaintiffs remain suspended from government contracting.[27] To date, their suspension has been in effect for thirty-one months.

3. Plaintiffs' attempts to have their suspensions terminated

In November of 2010, DGS retained the services of Contractor Integrity Solutions, L.L.C., to act as in independent consultant, beginning in 2011.[28] The purpose of the consulting agreement was to bolster the compliance system DGS already had in place.[29] On the basis of the consulting agreement, DGS wrote to the Agency, and made an oral presentation, asking for the Agency to reconsider its suspension.[30] The Agency denied that request, on the basis that it did not reflect "material information about a change in the relationship between DGS, Inc. and

---

[26] Certified Administrative Record, at Bates 623-728 (TRO Hearing Transcript); Certified Administrative Record, at Bates 1372-87 (Bench Ruling Transcript).

[27] Doc. no. 6-1 (Affidavit of Richard Brooks).

[28] Certified Administrative Record, at Bates 1706-08 (Engagement Letters).

[29] *Id.*

[30] *Cf.* Certified Administrative Record, at Bates 1710 (Letter Responding to Request for Reconsideration).

PWC."[31]

In June of 2011, after the suspension had been in effect for more than eighteen months, plaintiffs presented the Defense Logistics Agency the terms of a proposed "management buyout" of Agility.[32] Under the terms of that proposal, management employees of Agility would form a new holding company.[33] Those personnel would also resign their positions with PWC.[34] The new company would then buy a 60% stake of Agility from DGS.[35] PWC would ultimately retain a 40% stake in Agility through its indirect ownership of DGS, but the majority stake in the company would be held by the new company, whose employees would no longer be subject to PWC control. Moreover, PWC would not have any voting or management authority over Agility while PWC remained suspended.[36] Although the management buyout would have eliminated the formal control PWC previously held over Agility, the Agency informed plaintiffs that effecting the buyout would not terminate the suspension of Agility.[37] Accordingly, plaintiffs did not conduct the management buyout.

---

[31] *Id.*

[32] Complaint, at Ex. 4 (Management Buyout Term Sheet).

[33] *Id.* at 1.

[34] Certified Administrative Record, at Bates 1739 (Presentation of Management Buyout Terms to the Agency).

[35] Management Buyout Term Sheet, at 1.

[36] *Id.* at 2.

[37] Certified Administrative Record, at Bates 1755-56 (Letter in Response to Management Buyout Proposal). Chadick informed plaintiffs that "it is not in the best interests of the Government to do business with any PWC . . . affiliate or subsidiary, regardless of the equity interest, until the

Although the Agency rejected plaintiffs' proposed management buyout, it lifted the suspensions of other PWC subsidiaries in response to similar arrangements. At least two other companies had their suspensions terminated because they ceased to be affiliated with PWC. A company called LA3P was removed from the Excluded Parties List on December 17, 2009, "[b]ased on removing all management and operational control over LA3P from" DGS.[38] Another company, AFH Fuel Services, L.L.C., had its suspension lifted on September 15, 2010.[39] The suspension was terminated due to a change in the operating agreement governing the company.[40] Under the initial operating agreement, DGS had a minority ownership stake of 44%, and the authority to appoint one of the three "Managers" of the company.[41] Under the amended operating agreement, DGS maintained its ownership stake, but not its ability to appoint a Manager.[42]

Plaintiffs brought this action for injunctive and declaratory relief, seeking to

---

criminal case has been concluded." *Id.* at Bates 1756.

[38] Certified Administrative Record, at Bates 1395 (Termination of Suspension Letter, LA3P). The record does not indicate how that change was brought about.

[39] Certified Administrative Record, at Bates 1670 (Termination of Suspension Letter, AFH Fuel Services, L.L.C.).

[40] *Id.*

[41] *Cf.* Certified Administrative Record, at Bates 1656 (Letter of Counsel). The record does not actually contain the operating agreement under which DGS had that authority. However, the letter of counsel, and the amended operating agreements, demonstrate what the prior arrangement must have been.

[42] Certified Administrative Record, at Bates 1662-69 (Amended Operating Agreement).

have the suspension lifted. At present, the prosecution of PWC is ongoing, but no allegations of any wrongdoing have ever been leveled againts either plaintiff.

III. DISCUSSION

Plaintiffs present four counts in their complaint. The first three counts are based upon the Administrative Procedure Act. In the first count, plaintiffs allege that the Defense Logistics Agency has provided an inadequate rationale for the suspensions. In the second count, plaintiffs allege that the suspensions are punitive. And in the third, they argue that the suspensions are excessive in duration. In the fourth count, plaintiffs allege that the continuing suspensions violate the Due Process Clause of the Fifth Amendment to the United States Constitution.

A. The Administrative Procedure Act

The Administrative Procedure Act ("APA") provides that, when reviewing the action of an administrative agency, a court shall "hold unlawful and set aside agency action, findings, and conclusions found to be . . . arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law . . . ." 5 U.S.C. § 706(2)(A). Under that standard, a court's review of an agency decision is deferential, even at the summary judgment stage. *Kirkpatrick v. White*, 351 F. Supp. 2d 1261, 1270 (N.D. Ala. 2004) (citing *Preserve Endangered Area's of Cobb's History, Inc. v. U.S. Army Corps of Engineers*, 87 F.3d 1242, 1246 (11th Cir. 1996)). "To prove an agency's

decision was arbitrary and capricious, the challenging party must show the record is devoid of reasonable evidence supporting the agency's decision." *Id.* (citing *Organized Fishermen of Florida v. Franklin*, 846 F. Supp. 1569, 1573 (S.D. Fla. 1994)).

B. Justiciability of Plaintiffs' Claims

Defendants argue that the decision of the Agency to suspend plaintiffs, and to continue to hold them suspended, is not justiciable because those decisions are "committed to agency discretion by law." 5 U.S.C. § 701(a)(2). An agency decision is considered to fall within that exception to judicial review "if the statute is drawn so that a court would have no meaningful standard against which to judge the agency's exercise of discretion." *Heckler v. Chaney*, 470 U.S. 821, 830 (1985). Defendants argue that, because the regulation governing suspension states that an agency "may" extend the suspension to an affiliate of the wrongdoer, there are "no substantive guidelines, requirements, or criteria by which to measure whether an agency abused or did not abuse its discretion."[43] Even so, plaintiffs have been able to identify cases that demonstrate that the debarment or suspension of an affiliate, not itself accused of wrongdoing, presents a justiciable controversy. *See Cailoa v. Carroll*, 851 F.2d 395 (D.C. Cir. 1988) (reviewing and reversing suspensions of individuals alleged to be

[43] Doc. no. 10 (Brief in Support of Defendants' Motion for Summary Judgment and in Opposition to Plaintiffs' Motion for Summary Judgment), at 14.

affiliates of a debarred contractor). *Cf. Gonzalez v. Freeman*, 334 F.2d 570, 574-75 (D.C. Cir. 1964) ("An allegation of facts which reveal an absence of legal authority or basic fairness in the method of imposing debarment presents a justiciable controversy in our view."). Thus, the court concludes that plaintiffs do present justiciable claims, and turns to the merits of those claims.

C. Rationale for Initial Suspension

Resolution of plaintiffs' APA claims turns on the interpretation accorded to certain provisions of the Federal Acquisition Regulations System. In the first count of their complaint, plaintiffs allege that their suspension was not based on an adequate rationale and was, therefore, in violation of the APA.[44] The regulations provide that, "[t]he suspending official may, in the public interest, suspend a contractor for any of the causes in 9.407-2, using the procedures in 9.407-3." 48 C.F.R. § 9.407-1(a)-(b)(1). Section 9.407-2 enumerates nine offenses that serve as causes for suspension, such as fraud, bribery, antitrust violations, and commission of "other offense[s] indicating a lack of business integrity or business honesty." *Id.* § 9.407-2(9). Suspension of an individual contractor can lead to the suspension of others:

> Suspension constitutes suspension of all divisions or other organizational elements of the contractor, unless the suspension decision is limited by its terms to specific divisions, organizational elements, or commodities. *The suspending official may extend the suspension decision to include*

[44] *See* doc. no. 1 ¶¶ 51-61.

> *any affiliates of the contractor if they are* (1) specifically named and (2) given written notice of the suspension and an opportunity to respond (see 9.407-3(c)).

Id. § 9.407-1(c) (emphasis supplied). That is, "affiliates" are not automatically considered suspended, but may be suspended based on the notice and response procedures found in § 9.407-3(c). The regulations include a definition of "affiliates."

> Business concerns, organizations, or individuals are affiliates of each other if, directly or indirectly, (1) either one controls or has the power to control the other, or (2) a third party controls or has the power to control both. Indicia of control include, but are not limited to, interlocking management or ownership, . . . shared facilities and equipment, [and] common use of employees . . . .

Id. § 9.403.

There is no dispute that, through indirect ownership of several subsidiaries, plaintiffs are "affiliates" of PWC, as defined in the regulations. The regulatory language clearly allows for the suspension of affiliates without any allegations of wrongdoing against them. The suspending official has the power to "extend" the suspension to them, and is required only to specifically name the affiliate and provide it with notice and an opportunity to respond. To require a finding, or even an allegation, of wrongdoing, would render the language of § 9.407-1(c) surplusage. That is, there would be no need for a provision specifically addressing the suspension of an affiliate if the government was required to apply the same procedures to affiliates as to principals. Judge Roberts reached the same conclusion when plaintiffs

attempted to enjoin their suspension at the outset, stating that "if the determination necessary to suspend the contractor in the first instance and an affiliate of that contractor were the same, it might render Section 9.407(c) a nullity."[45] Judge Roberts continued:

> [T]here must be some difference in the findings necessary to suspend a contractor in the first instance and to suspend an affiliate of that contractor. That difference appears to be that Section 9.407-1(c) authorizes a suspending official to suspend an affiliate on the basis of finding the affiliation alone without a finding of culpability.[46]

This court finds Judge Roberts's rationale persuasive, and concludes that the initial suspension of plaintiffs, as affiliates of PWC, was valid.

D. Excessive Duration of Suspension

The third count of plaintiffs' alleges that their suspension violates the APA because it has continued for a period greater than eighteen months.[47] Although the plain language of the regulations supports the validity of the initial decision by the Agency to suspend plaintiffs' contracting privileges, the question of the indeterminate duration of that suspension is murkier. The regulatory language regarding the duration of suspension does not draw a clear distinction between the suspensions of

---

[45] Bench Ruling Transcript, at Bates 1380.

[46] *Id.* at Bates 1380-81.

[47] *See* doc. no. 1 ¶¶ 66-74. As noted in the beginning of Part III of this opinion, the second count of plaintiffs' complaint alleges that their continued suspension is "punitive." *Id.* ¶¶ 62-65. Consideration of that claim is rendered moot by the following discussion and resolution of the claim asserted in the third count.

principals and affiliates, nor does it clearly treat them alike. The relevant part of the regulation reads as follows:

> If legal proceedings are not initiated within 12 months after the date of the suspension notice, the suspension shall be terminated unless an Assistant Attorney General requests its extension, in which case it may be extended for an additional 6 months. In no event may a suspension extend beyond 18 months, *unless legal proceedings have been initiated within that period*.

48 C.F.R. § 9.407-4(b) (emphasis supplied). The last sentence of that provision provides the nub of disagreement between the parties. Defendants argue that legal proceedings against the suspended principal contractor allow the continued suspension of its affiliates. In other words, they read the sentence as providing that: "In no event may a suspension *of an affiliate* extend beyond 18 months, unless legal proceedings have been initiated *against the principal* within that period." Conversely, plaintiffs argue that legal proceedings must be initiated against the affiliate itself for the suspension to continue. That is, they read the sentence to as saying that: "In no event may a suspension *of an affiliate* extend beyond 18 months, unless legal proceedings have been initiated *against the affiliate itself* within that period."

The pivotal issue of whether the suspension of an affiliate may extend beyond 18 months merely on the basis of legal proceedings being brought against the principal appears to be unsettled. The parties have not identified a single judicial decision addressing the issue, nor has the court's independent research discovered

any.[48] Defendants argue that the regulation allows for the indefinite suspension of an affiliate, because to hold otherwise "would lead to absurd and illogical results," which regulations should be interpreted to avoid. *See, e.g.*, *Rhode Island Hospital v. Leavitt*, 548 F.3d 29, 37 (1st Cir. 2008). Plaintiffs argue that to allow indefinite suspension on the basis of affiliation alone would contradict the "structure" of the regulation.

1. Arguments of the parties

Defendants note that subsidiaries may be initially suspended on the sole basis of their affiliation with a parent company accused of impropriety. They argue that, "if suspension is based on affiliation, it is only logical that the period of suspension for the affiliate should be the same as for the primary contractor."[49] They state that "[o]ne purpose for suspending affiliates is to prevent the primary contractor from shifting business to its affiliates, thereby allowing the affiliates to bid on government contracts and avoid the consequences of suspension from government contracting."[50] Defendants further argue that, if affiliation-based suspensions were limited to eighteen months, a suspended contractor could create new subsidiaries to sidestep suspension. After eighteen months, those new subsidiaries, which did not exist at the time of the

---

[48] In fact, electronic searches of the West and Lexis databases returned only six cases in which § 9.407-4 is mentioned at all, none of which address the question before the court.

[49] Doc. no. 15 (Reply Brief in Support of Defendants' Motion for Summary Judgment and in Opposition to Plaintiffs' Motion for Summary Judgment), at 7.

[50] *Id.* at 4.

events leading to indictment of their parent, would be eligible for contracting. The suspended parent would profit from the subsidiaries' contracts. That result, say defendants, would be absurd. They argue that it is only logical that a suspension on the basis of affiliation should last as long as the suspension of the primary contractor, and state that this is what occurs in practice.

Rather than hypothecating circumstances under which primary how contractors might abuse the system, plaintiffs focus their arguments on the text of the regulation itself. Plaintiffs point out the distinctions between the language of § 9.407-1 and that of § 9.407-4. The former section establishes two bases for suspension: suspicion of any of the offenses listed in § 9.407-2, or affiliation with a contractor suspected of any of the offenses listed in § 9.407-2. 48 C.F.R. § 9.407-1(a), (c).[51] Conversely, § 9.407-4 simply states that a suspension may not last longer than eighteen months, "unless

---

[51] The full text of those subsections reads as follows:

> (a) The suspending official may, in the public interest, suspend a contractor for any of the causes in 9.407–2, using the procedures in 9.407–3.
>
> . . .
>
> (c) Suspension constitutes suspension of all divisions or other organizational elements of the contractor, unless the suspension decision is limited by its terms to specific divisions, organizational elements, or commodities. The suspending official may extend the suspension decision to include any affiliates of the contractor if they are (1) specifically named and (2) given written notice of the suspension and an opportunity to respond (see 9.407–3(c)).

48 C.F.R. § 9.407-1(a), (c).

legal proceedings have been initiated within that period." *Id.* § 9.407-4(b).[52] That section makes no distinction between suspensions on the basis on an enumerated cause and those on the basis of affiliation. Thus, argue plaintiffs, all suspended contractors must be treated equally under that provision, and cannot be suspended for longer than eighteen months unless legal proceedings have been brought against them.

2. Analysis

Plaintiffs' interpretation, based on the text of the regulation itself, is sounder. Although the regulation establishes two different methods of commencing suspension, it contains only one provision regarding the expiration of suspension. That one provision must be applied to suspected wrongdoers and suspended affiliates in a consistent manner. Defendants' concern that plaintiffs' interpretation produces absurd results is mitigated by several factors. Although defendants state that one reason the regulation allows for the suspension of affiliates is to prevent the primary contractor from shifting business to them, that is but *one* reason.

Another equally plausible reason is to allow the government adequate time to

---

[52] The full text of § 9.407-4(b) provides:

> If legal proceedings are not initiated within 12 months after the date of the suspension notice, the suspension shall be terminated unless an Assistant Attorney General requests its extension, in which case it may be extended for an additional 6 months. In no event may a suspension extend beyond 18 months, unless legal proceedings have been initiated within that period.

48 C.F.R. § 9.407-4(b).

investigate the affiliates for wrongdoing on their own part. That purpose becomes clear when § 9.407-1 and § 9.407-4 are read in conjunction; the government may immediately suspend numerous affiliates on the basis of its suspicion of one of them, and then has a limited period of time in which to determine which affiliates *actually* participated in wrongdoing before it must terminate the suspensions of those not facing accusations. That arrangement allows the government to put an immediate stop to potential wrongdoing that it may not have been able to investigate fully, but it does not give the government the power to suspend an affiliate *indefinitely* without even *suspicion* of wrongdoing. When the investigative purpose of the affiliation-based suspension is considered, the fundamental flaw in defendants' interpretation is revealed. That interpretation would allow the government to issue a blanket suspension against numerous contractors and, so long as proceedings were initiated against one of them, allow the government to sit on its hands, rather than taking steps to investigate and determine within a reasonable period of time whether the affiliates were guilty of misconduct, all while those affiliates suffered the loss of business.[53]

Another flaw in defendants' argument is exposed upon a close reading of the regulatory definition of "affiliate." Defendants' argument is premised on the idea that

[53] Because the court finds that plaintiffs' interpretation of the statutory language is correct, it need not address the question of whether defendants' interpretation violates the Due Process Clause. However, to allow the government to suspend a contractor indefinitely, without suspicion, raises due process concerns.

"affiliates" will necessarily be subsidiaries of the "primary" contractor, which will be their parent company. That is, in fact, the scenario here. However, "affiliate" is defined more broadly. Although "control" is integral to the definition, both the parent and the subsidiary are considered affiliates of each other. 48 C.F.R. § 9.403 ("Business concerns, organizations, or individuals *are affiliates of each other* if, directly or indirectly, (1) either one controls or has the power to control the other, or (2) a third party controls or has the power to control both.") (emphasis supplied). Thus, the regulation allows for the suspension of a parent company for the malefactions of its subsidiary, on the mere basis that the parent company is an affiliate of the subsidiary. In such a scenario, the danger of a "primary" contractor shifting business to its "affiliates" and, thereby, circumventing the consequences of suspension would seem to be much reduced.

In addition to the possibility that a contractor will shift business to its subsidiaries if they are not suspended, defendants hypothesize that a suspended contractor could create new, wholly-owned subsidiaries in the wake of a suspension. Because those companies did not previously exist, they could not be tainted with the wrongdoing that led to the suspension of the primary contractor. Defendants argue that an eighteen month cap on affiliation-based suspensions would allow a suspended contractor to use such wholly-owned subsidiaries to engage in unfettered contracting.

That argument is seriously undermined by the regulatory scheme. In addition to the nine offenses enumerated as cause for suspension in § 9.407-2, there is a catchall provision: "The suspending official may upon adequate evidence also suspend a contractor for any other cause of so serious or compelling a nature that it affects the present responsibility of a Government contractor or subcontractor." 48 C.F.R. § 9.407-2(c). The creation of wholly-owned subsidiaries in order to circumvent a suspension arguably fits within that catchall provision. Thus, plaintiffs' interpretation of the regulation would not, as defendants assert, amount to *carte blanche* for suspended contractors seeking to continue to profit from government contracting, as the government would have cause to suspend new subsidiaries created for the purpose of abusing the system.

Finally, the language of the catchall provision highlights another regulatory requirement that also protects the government from unscrupulous contractors. Before considering any bid for a contract, the government must determine whether the bidder is presently "responsible." *See* 48 C.F.R. § 9.103. "No purchase or award shall be made unless the contracting officer makes an affirmative determination of responsibility. In the absence of information clearly indicating that the prospective contractor is responsible, the contracting officer shall make a determination of nonresponsibility." *Id.* § 9.103(b). To be found responsible, a contractor must have,

among other things "a satisfactory record of integrity and business ethics . . . ." *Id.* § 9.104-1(d). The determination of responsibility must be made anew for each potential contract. *See OSG Product Tankers, L.L.C. v. United States*, 82 Fed. Cl. 570, 575 (Fed. Cl. 2008); *Frequency Electronics, Inc. v. Department of the Air Force*, 151 F.3d 1029 (Table), No. 97-1551, 1998 WL 377929, at *2 (4th Cir. July 1, 1998) ("'Responsibility' is a present condition and not an indelible status."). The fact that a contractor is not suspended or debarred from contacting is no guarantee that it will be found presently responsible upon submitting a bid. A contractor that is a newly-created, wholly-owned subsidiary of a suspended contractor would surely raise a red flag in the process of determining present responsibility.

The court concludes that the interpretation of the regulation proposed by plaintiffs is the correct one. That is, no contractor may be suspended for greater than eighteen months unless legal proceedings are initiated against that contractor itself, regardless of the basis for the initial decision to suspend the company. The facts in the record are undisputed: plaintiffs were suspended on the sole basis of their affiliation with PWC; no legal proceedings have been initiated against them; and they have remained suspended for thirty-one months — *i.e.*, nearly twice the regulatory limit of eighteen months. Their continued suspension is contrary to law, in violation of the APA. Therefore, their suspensions must be terminated. Summary judgment is

due to be granted in favor of plaintiffs, and against defendants.

IV. ORDERS AND INJUNCTION

For the reasons stated herein, plaintiffs' motion for summary judgment is GRANTED, and defendants' motion for summary judgment is DENIED.

It is DECLARED that defendants' suspension of plaintiffs for greater than eighteen months, without the initiation of legal proceedings against plaintiffs, is contrary to law. Additionally, it is DECLARED that plaintiffs are eligible for government contracts, provided they are determined to meet the responsibility requirements of 48 C.F.R. § 9.103.

It is further ORDERED, ADJUDGED, and DECREED that defendants lift plaintiffs' suspension from government contracting, and remove them from the Excluded Parties List.

Costs are taxed to defendants. The clerk is directed to close this file.

DONE and ORDERED this 26th day of June, 2012.

United States District Judge

Agility Defense & Government Services
v.
United States

No. 13-10757

(11th Cir. Dec. 31, 2013)

[PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 13-10757

D.C. Docket No. 5:11-cv-04111-CLS

AGILITY DEFENSE & GOVERNMENT SERVICES,
AGILITY INTERNATIONAL, INC.,

Plaintiffs–Appellees,

versus

U.S. DEPARTMENT OF DEFENSE,
SECRETARY OF DEFENSE,
DEFENSE LOGISTICS AGENCY,
DIRECTOR OF THE DEFENSE LOGISTICS AGENCY,

Defendants–Appellants.

Appeal from the United States District Court
for the Northern District of Alabama

(December 31, 2013)

Before PRYOR and COX, Circuit Judges, and ROSENTHAL,[*] District Judge.

---

[*] Honorable Lee H. Rosenthal, United States District Judge for the Southern District of Texas, sitting by designation.

PRYOR, Circuit Judge:

This appeal requires us to decide whether a federal agency may suspend two affiliates of an indicted government contractor for the duration of the legal proceedings against the indicted contractor under the Federal Acquisition Regulation. See 48 C.F.R. § 9.407-4(b) (2012). When an agency suspends a government contractor, the agency may also suspend an affiliate of the contractor based solely on its affiliate status. Id. § 9.407-1(c). Suspensions are temporary, and in "no event may a suspension extend beyond 18 months, unless legal proceedings have been initiated within that period." Id. § 9.407-4(b). We must determine whether the term "legal proceedings," in this regulation, refers to proceedings against the indicted government contractor or against the suspended affiliates of that contractor. The district court interpreted the term to refer to proceedings against the suspended affiliates, not the indicted contractor, but we disagree. Because the suspension of an affiliate is "include[d]" as part of the suspension of the indicted government contractor, id. § 9.407-1(c), we conclude that legal proceedings initiated against the indicted government contractor tolled the 18-month time limit for the suspension of the affiliates. We reverse the summary judgment in favor of the affiliates and render a judgment in favor of the defendants.

I. BACKGROUND

The Federal Acquisition Regulation governs the acquisition of supplies and services by all federal agencies. See Establishing the Federal Acquisition Regulation, 48 Fed. Reg. 42,102-01-A (Sept. 19, 1983). For example, the regulation governs the contracts between the Department of Defense and the appellants, Agility Defense & Government Services and Agility International, Inc., which are government contractors. Under this regulation, a prospective government contractor must demonstrate its "responsibility" before an agency awards a government contract. 48 C.F.R. §§ 9.103, 9.104-1. When an existing contractor is deemed non-responsible, the regulation provides for the suspension and debarment of the non-responsible contractor and its affiliates. Id. §§ 9.406-2, 9.407-2.

An agency official may suspend a government contractor for various reasons, including the contractor's commission of fraud or a criminal offense, unfair trade practices, or "other offense[s] indicating a lack of business integrity or business honesty that seriously and directly affects the present responsibility of a Government contractor or subcontractor." Id. § 9.407-2(a). The agency official may extend the suspension of the indicted government contractor "to include any affiliate[] of the contractor if they are (1) specifically named and (2) given written notice of the suspension and an opportunity to respond." Id. § 9.407-1(c); see also

id. § 9.403 (defining "affiliate"). A suspension of an indicted government contractor and its affiliates is a "temporary" remedy to "protect the Government's interest." Id. §§ 9.407-4(a), 9.407-1(b)(1). And "[i]n no event may a suspension extend beyond 18 months, unless legal proceedings have been initiated within that period." Id. § 9.407-4(b).

Based on this regulation, Agility Defense and Agility International were suspended in November 2009. A grand jury indicted the parent company of Agility Defense and Agility International, Public Warehousing Company, K.S.C., for a multibillion-dollar fraud perpetrated against the United States in connection with its government contract to supply food to American military personnel in the Middle East. The Defense Logistics Agency, a combat support agency of the Department of Defense, suspended Public Warehousing on November 16, 2009, on the basis of the indictment. See id. § 9.407-1(c). On the same day, the agency extended the suspension to Agility Defense because it was an affiliate of Public Warehousing. And on November 23, 2009, the agency suspended Agility International on the same basis.

The affiliates submitted written responses in opposition to their suspensions. They argued that they were not implicated in the indictment of Public Warehousing and that they had sufficient compliance procedures to guard against fraud. The agency rejected their requests to terminate the suspensions. Both

affiliates then sought a temporary restraining order to enjoin the agency from implementing the suspensions, which the District Court for the District of Columbia denied.

The affiliates appealed to the agency to reconsider their suspensions, but the agency refused their requests. Agility Defense presented new evidence of improved compliance procedures, but the agency refused to terminate its suspension. The agency likewise refused to reconsider the suspension of Agility International after it proposed a management buyout, in which a new holding company would buy a 60-percent stake in Agility International, and Public Warehousing would indirectly retain only 40-percent ownership. The agency stated that the buyout would not affect its suspension, so Agility International did not complete the buyout.

After the agency lifted the suspensions of other affiliates of Public Warehousing based on similar management buyout plans, Agility Defense and Agility International filed this action for injunctive and declaratory relief. Both parties agreed that there was no genuine dispute as to any material fact and moved for summary judgment. The district court granted summary judgment in favor of the affiliates and denied summary judgment in favor of the agency. The district court ruled that the agency did not have the power to suspend the affiliates indefinitely even if it initially had the power to suspend the affiliates based solely

on their affiliate status. Because neither the United States nor its agencies initiated legal proceedings against the affiliates within 18 months of their suspension notices, the district court declared the suspensions contrary to law and ordered the agency to terminate the suspensions.

II. STANDARD OF REVIEW

We review a grant of summary judgment de novo. See Citizens for Smart Growth v. Sec'y of the Dep't of Transp., 669 F.3d 1203, 1210 (11th Cir. 2012). We apply the same legal standards as the district court when we review an agency action, and we set aside the agency action only if it is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with the law." Id.; see 5 U.S.C. § 706(2)(A).

III. DISCUSSION

We divide our discussion in two parts. First, we hold that the regulation permits the suspension of an affiliate of an indicted government contractor to exceed 18 months when legal proceedings have been initiated against the indicted government contractor. Second, we hold that the regulation does not unconstitutionally deprive the affiliates of their right of due process under the Fifth Amendment.

A. The Suspension of an Affiliate of an Indicted Government Contractor May Exceed 18 Months When Legal Proceedings Have Been Initiated Against the Indicted Government Contractor.

The central issue in this appeal is whether the United States or its agencies must initiate legal proceedings against an affiliate of an indicted government contractor to toll the 18-month time limit on the suspension of the affiliate even though the affiliate was suspended solely on account of its affiliate status. The regulation states, "In no event may a suspension extend beyond 18 months, unless legal proceedings have been initiated within that period." 48 C.F.R. § 9.407-4(b). The agency argues that we must interpret "legal proceedings" as legal proceedings against the indicted government contractor. The affiliates argue that we must interpret "legal proceedings" as legal proceedings against the suspended affiliate of the indicted government contractor. We agree with the agency.

We interpret the term "legal proceedings" in context with two related provisions in the regulation. See FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 132–33, 120 S. Ct. 1291, 1301 (2000) ("The meaning—or ambiguity—of certain words or phrases may only become evident when placed in context."); Strickland v. Water Works and Sewer Bd. of City of Birmingham, 239 F.3d 1199, 1204–05 (11th Cir. 2001); see also Antonin Scalia & Bryan A. Garner, Reading Law: The Interpretation of Legal Texts 167–69 (2012) ("The text must be construed as a whole."). First, the regulation clearly states that an agency can

suspend an affiliate based solely on its status as an affiliate of an indicted government contractor. 48 C.F.R. § 9.407-1(c). Second, the parallel provision governing debarment likewise permits an affiliate to be debarred solely based on its status as an affiliate. Id. § 9.406-1(b). Together, these provisions make clear that the suspension and debarment of an affiliate derive solely from its status as an affiliate; no showing of wrongdoing by the affiliate is required for suspension or debarment.

Because the regulation clearly establishes that the agency can suspend an affiliate without any showing of wrongdoing by the affiliate, we read "legal proceedings" as legal proceedings against the indicted government contractor. The agency must satisfy only three requirements to suspend an affiliate: (1) it must establish that the affiliate has the power to control the indicted government contractor or be controlled by the indicted government contractor; (2) it must specifically name the affiliate; and (3) it must provide notice of the suspension and notice of an opportunity for the affiliate to respond. Id. §§ 9.403, 9.407-1(c). Together, the suspensions of an indicted government contractor and its affiliate constitute one "suspension decision" because an affiliate is "include[d]" in the suspension of the indicted government contractor. Id. § 9.407-1(c). No cause precipitates the suspension of an affiliate except for its association with the indicted government contractor. The United States and its agencies have little

reason to initiate legal proceedings against an affiliate suspended solely on account of its affiliate status.

The affiliates argue that an affiliate must be treated as an independent entity when an agency evaluates the duration of its suspension because an agency treats an affiliate as an independent entity when evaluating whether the affiliate is eligible to be a government contractor. See id. § 9.104-3(c). But the agency action before us is not a finding of present responsibility for the purpose of awarding a government contract. We are instead reviewing the suspensions of two affiliates, which all parties agree derive solely from their association with Public Warehousing following its indictment for a multibillion-dollar fraud committed against the United States. The whole text of the regulation provides that an affiliate can be suspended based solely on its affiliate status so long as the agency establishes that it is an affiliate, gives notice of the suspension, and provides an opportunity to respond to the suspension. The present responsibility of an affiliate is irrelevant.

We also read the disputed text in context with the parallel provision of the regulation governing debarment. A suspension is the precursor to the more permanent remedy of debarment. See id. § 9.406-1. If the prosecution of a government contractor results in a conviction, for example, then that conviction can serve as the basis to debar the contractor. The agency may also debar an

affiliate of that contractor based solely on its affiliate status. Id. § 9.406-1(b). Like suspensions, an agency can debar an affiliate even if the affiliate has not engaged in wrongdoing. Id. § 9.406-1(b); see also Leitman v. McAusland, 934 F.2d 46, 48, 48 n.2 (4th Cir. 1991); Robinson v. Cheney, 876 F.2d 152, 154 (D.C. Cir. 1989); Ciaola v. Carroll, 851 F.2d 395, 400 (D.C. Cir. 1988). Only one court has stated that the debarred affiliate "must have been involved in or affected by the contractor's wrongdoing to be named in the debarment," OSG Prod. Tankers LLC v. United States, 82 Fed. Cl. 570, 578 (2008), but this statement by the Court of Federal Claims was dicta. OSG Product Tankers involved a dispute about whether the company was eligible to be a government contractor, and the opinion included discussion of a previous debarment. This dicta about a requirement of wrongdoing by the affiliate in OSG Product Tankers is unpersuasive in the light of the whole text of the regulation and the decisions of our sister circuits, which allow the debarment of an affiliate based solely on its status as an affiliate.

Our reading of the provisions governing debarment makes sense of the term "legal proceedings" in the provision governing suspension. If the legal proceedings against Public Warehousing were to result in a conviction and debarment, the agency could debar both Agility Defense and Agility International based solely on that conviction and debarment of Public Warehousing. It would be nonsensical to require the agency either to terminate the suspensions of the

affiliates or to initiate separate legal proceedings against the affiliates, only to debar them if the legal proceedings against Public Warehousing end in a conviction.

B. A Suspension of an Affiliate that Exceeds 18 Months Is Not a Violation of Due Process Because the Regulation Affords an Affiliate Constitutionally Sufficient Process To Contest Its Suspension.

To establish a violation of the Due Process Clause of the Fifth Amendment, the affiliates must prove that they have a constitutionally protected interest in liberty or property, that the government deprived them of that interest, and that the procedures accompanying that deprivation are constitutionally inadequate. See Bank of Jackson Cnty. v. Cherry, 980 F.2d 1362, 1366 (11th Cir. 1993). A contractor possesses no property interest in doing business with the United States. Id. But a contractor can establish that an agency deprived it of its liberty interest if it proves that an agency has made a stigmatizing allegation, the allegation has been disseminated or publicized, and the allegation has resulted in the loss of a tangible interest. Id. at 1367.

The district court erred when it stated that the suspensions of the affiliates, which exceeded 18 months, "raise[d] due process concerns" because the regulation guarantees constitutionally adequate process. It is unlikely that the regulation infringes on the liberty interests of the affiliates given that their suspensions were predicated solely on their status as affiliates of Public Warehousing and the agency

did not make any allegations of wrongdoing against them. But, even assuming that the suspension of the affiliates deprived them of their liberty, the regulation does not violate the Due Process Clause because it contains constitutionally adequate procedures. An agency must immediately notify a suspended affiliate of its suspension by certified mail. 48 C.F.R. § 9.407-3(c). That notification includes the basis of the suspension and advises the affiliate of its opportunity to respond in writing. Id. These procedures—notification and an opportunity to respond—are constitutionally adequate procedures for multiyear suspensions. See Home Bros., Inc. v. Laird, 463 F.2d 1268, 1271 (D.C. Cir. 1972) ("[A]n action that 'suspends' a contractor and contemplates that he may dangle in suspension for a period of one year or more . . . . requires that the bidder be given specific notice as to at least some charges alleged against him, and be given, in the usual case, an opportunity to rebut those charges.").

The affiliates contend that the continuation of their suspensions without additional process is "constitutionally dubious," but the affiliates fail to recognize that the agency afforded them additional process when it twice considered their request to terminate their suspensions. In both instances, the agency ruled that the affiliates could not establish that they were no longer "affiliates" of Public Warehousing. See 48 C.F.R. § 9.403. So long as they are affiliates of Public Warehousing, they can be suspended. See id. § 9.407-1(c). The affiliates have

conflated constitutionally adequate process with getting their way. That the agency refused to lift their suspensions is not the equivalent of constitutionally inadequate process.

IV. CONCLUSION

We **REVERSE** the summary judgment in favor of the affiliates, Agility Defense and Agility International, and **RENDER** a judgment in favor of the defendants.

Strategies for Managing & Mitigating Risk in Government Contracts

11:00 a.m. – 12:00 p.m.

Thomas Barrett, KBR

James Y. Boland, Venable LLP

Paul A. Debolt, Venable LLP

Rodney W. Mateer, Deloitte Financial Advisory Services LLP

William L. Walsh, Jr., Venable LLP

VENABLE® LLP

VENABLE® LLP

Strategies for Managing & Mitigating Risk in Government Contracts

APRIL 10, 2014

VENABLE® LLP

Venable Government Contracts Symposium

Strategies for Managing & Mitigating Risk in Government Contracts

Moderator:

Bill Walsh
Government Contracts Practice Group, Venable LLP

Panelists:

Thomas J. Barrett
Chief Legal Officer, KBR – North American Government & Logistics

Rodney W. Mateer
Director, Deloitte Financial Advisory Services LLP

Paul Debolt
Government Contracts Practice Group, Venable LLP

James Boland
Government Contracts Practice Group, Venable LLP

Biographies

William L. Walsh, Venable LLP

Bill Walsh concentrates his practice on representing federal sector companies who contract with DOD and civilian agencies. He represents clients locally, nationally, and internationally in issues including dispute resolution (ADR) and bid protests before the U.S. Government Accountability Office, Federal Boards of Contract Appeals, and executive agencies on contract administration matters, contract claims, contract terminations, teaming agreements, contractor qualification issues, organizational and personal conflict of interest concerns and small business matters.

Mr. Walsh has 30 years of federal and state government contract experience and extensive knowledge and skills in this complex area. Mr. Walsh's legal career began as a lawyer with the DOD on government contract and legislative issues. Mr. Walsh also served as Chief Counsel for NASA's Marshall Space Flight Center.

In the past few years, in addition to assisting several clients in pursuing protest claims before the Government Accountability Office, Mr. Walsh has also represented clients with claims before the Armed Services Board of Contract Appeals. He usually serves as lead counsel on numerous significant protest matters involving, collectively, several billion dollars in contract value. He has also managed several substantial prime-subcontractor disputes as well as a number of suspension/debarment matters and related civil false claims matters.

Panelist Biographies

Thomas J. Barrett
Chief Legal Officer, KBR – North American Government & Logistics

Tom Barrett is the Chief Legal Officer for KBR's North American Government & Logistics business unit offering world-wide logistics, operation and maintenance, construction, and services to numerous U.S. and foreign government entities, and various domestic and international companies. Tom has many years of experience both in the government and the private sector providing legal services and business advice regarding government contract, fiscal, administrative, military, operational, logistics, and construction law, government compliance, and complex civil and criminal litigation. Previously, Mr. Barrett was the Senior Counsel for KBR's Design and Construction Product Line, and the Theater Deputy Government Compliance Manager in Iraq.

Prior to joining KBR, Mr. Barrett served as a member of the U.S. Army Judge Advocate General's Corps retiring from active duty in early 2007. Tom received his B.A. in Political Science from Fairfield University, his J.D. from the Marshall-Wythe School of Law, The College of William and Mary, and his L.L.M. in Military Law (Contract and Fiscal Law) from the U.S. Army Judge Advocate General's School. Mr. Barrett is also a graduate of the U.S. Navy Nuclear Power Program serving in the submarine service, and later worked as a high-energy microwave R&D engineering assistant for Cober Electronics, Inc.

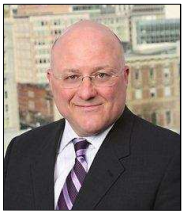
Panelist Biographies

Rodney W. Mateer,
Director, Deloitte Financial Advisory Services LLP

Mr. Mateer is a Director of the Deloitte Financial Advisory Services LLP ("Deloitte FAS") government contracting regulatory and compliance practice. With over 35 years of experience, he specializes in government contract cost accounting, audit and regulatory matters relating to the Federal Acquisition Regulation (FAR), Cost Accounting Standards (CAS), Truth-in-Negotiations Act (TINA), and OMB Circulars. Mr. Mateer represents contractors in such areas as FAR/CAS compliance, business system compliance readiness, claim/proposal preparation, merger and acquisition due diligence, defective pricing, litigation support, and analysis/damage assessment of alleged violations of the civil False Claims Act. He lectures and authors articles on government contract cost issues, and is a member of several professional associations. Mr. Mateer is a Certified Public Accountant and a member of the Virginia State Bar.

Panelist Biographies

Paul A. Debolt, Venable LLP



Paul Debolt assists companies and individuals on issues that arise from conducting business with the federal government, including civil fraud. He is experienced in the competitive source selection process, defending or prosecuting bid protests, issuing advice concerning compliance with government regulations and laws during the performance of a contract, and helping to resolve disputes and claims during contract performance or as a result of contract termination. Mr. Debolt also counsels clients on the Service Contract Act, the civil False Claims Act, joint ventures and teaming agreements, prime-subcontractor disputes, internal investigations, mandatory disclosures and data rights issues.

Mr. Debolt has extensive government contracts law experience and applies a team approach that ensures clients receive the benefit of firm-wide strength in all related areas.

Panelist Biographies

James Y. Boland, Venable LLP

James Boland is a member of the firm's Government Contracts Group. Mr. Boland's practice covers a broad range of federal procurement counseling and litigation, including bid protests; claims and requests for equitable adjustments; Federal Circuit appeals; prime/subcontractor agreements and disputes; small business matters; teaming and joint venture agreements; suspension and debarment; compliance and internal investigations; security clearance appeals; and intellectual property issues.

Mr. Boland also advises clients in the pre- and post-award source selection stages of procurements. He has successfully challenged and defended solicitations, evaluations, contract award decisions, and offeror size/status eligibility before numerous defense and civilian agencies, the Government Accountability Office, the Small Business Administration, the United States Court of Federal Claims, and the FAA's Office of Dispute Resolution for Acquisition. In addition, Mr. Boland prepares, negotiates and litigates a wide variety of claims under the Contract Disputes Act before the Armed Services and Civilian Boards of Contract Appeals and the United States Court of Federal Claims, including claims for: equitable adjustments based on contract changes, breach of contract damages, Prompt Payment Act interest and penalties, misappropriation of trade secrets and intellectual property, and claims arising out of terminations for default and convenience.

Agenda

- Types of Risk
- Managing Risk During RFP & Contract Formation
- Mitigating Risk at the Contract's Outset
- Managing Risk During Contract Administration
- The Civil False Claims Act
- Contract Litigation

Types of Risk

- Performance Risk
- Contractual Risk
- Financial Risk
- Litigation Risk

Performance Risk

- The risk that the contractor will not successfully complete the contract.
  - Failure to perform the contract within the allotted schedule
  - Failure to produce conforming goods

Contractual Risk

- The risk that the contractor's rights and duties may be different than anticipated at the contract's outset.
  - Requirement to perform additional obligations that were not anticipated at the contract's outset
  - Inspections
  - SCA wages
  - New (and/or changing) regulations
  - Varying contract interpretations

Financial Risk

- The risk that a contractor will not optimize its profit or that it will suffer unanticipated losses.

VENABLE LLP

Managing Risk in Government Contracts

VENABLE LLP

Three Stages of Risk Management

- Contract Formation
- Contract Administration
- Contract Litigation

VENABLE LLP

Managing Risk During RFP & Contract Formation

- Identifying and managing risk at the outset of the RFP and contract is the contractor's best opportunity to ensure successful performance.
- Contractors must understand the scope of work.
- Contractors must understand the risk associated with performance and factor this into their bid and performance plan.

VENABLE LLP

Understanding the Scope of Work

Key Questions to Ask in the RFP Stage:

- Does the RFP/contract clearly define what the contractor is required to do?
  - PWS, FAR Clauses, Deliverables
- What are the metrics for determining successful performance?
  - Objective vs. Subjective Measurements
- How easily can requirements change?
  - Understand the difference between FAR 52.212-4(c) and FAR 52.243-1
- What are the potential liabilities?
  - Default/Cause, Excess Re-procurement (FAR 52.249-8; 52.212-4(m))
  - Indemnity (*e.g.*, Patent Indemnity, FAR 52.212-4(h))

Mitigating Risk

- Actively Participate in the Pre-Solicitation Phase
  - Take RFIs seriously
  - Help the agency define T&Cs and schedule acceptable to the industry
  - Explain why proposed terms are not feasible or too risky
- Ask Detailed Questions in the Solicitation Phase
  - Force the agency to commit to certain contract interpretations
  - Request that the agency make changes, and explain why current terms are not workable
- No RFP is Perfect; Factor Acceptable Risks into Price

Mitigating Risk

- Consider if the Risk is so Great it Warrants a Pre-Award Protest
  - *U.S. Foodservice, Inc. v. United States*, 100 Fed. Cl. 659 (2011)
  - *CW Government Travel, Inc. v. United States*, 99 Fed. Cl. 666 (2011)
  - *CWTSatoTravel*, B-404479.2, 2011 CPD ¶ 87
- Secondary Benefit of Filing a Pre-Award Protest is Committing the Agency to Take a Firm Position

VENABLE LLP

Managing Risk During Contract Administration

VENABLE LLP

Contract Administration

- Continually Monitor Performance, Cost and Schedule
  - Maintain dialogue with the CO
  - Advise the CO early and often if likely to encounter problems and work out a solution before potential non-performance, or defective performance
  - Nobody wants litigation, but operate as though you will litigate

Contract Administration

Who has contractual authority?

- "Where a party contracts with the government, apparent authority of the government's agent to modify the contract is not sufficient; an agent must have actual [express or implied] authority to bind the government."

Winter v. Cath-Dr/Balti JV, 497 F.3d 1339 (Fed. Cir. 2007)

- Are oral instructions sufficient?

GarCom, Inc., ASBCA No. 55034, 06-1 BCA ¶ 33,146 (Board denied a contractor's claim alleging that the government representative's instructions led it to exclude business privilege taxes from its proposal, where the solicitation required that all questions be in writing, the contractor knew the contract included a clause making it responsible for all taxes, and the contractor unreasonably relied on oral instructions from the government representative.)

Contract Administration

Who has contractual authority?

- What is the extent of the COTR's authority?

Nu-Way Concrete Co., Inc. v. Dept. of Homeland Security, CBCA No.1411,11-1 BCA ¶ 34,636 (Board held that contractor "failed to show by a preponderance of the evidence that the Government ordered it to perform work beyond that required by the contract" because inspectors did not have actual authority.)

Southwestern Security Services v. Dept. of Homeland Security, CBCA No. 1264, 09-2 BCA ¶ 34,139 (Board held that the COTR did not have the authority to bind the government under a separate contract, and thus, the contractor "should have investigated further into the issue of authority when it believed that it was entering into a separate contract" with the COTR.)

- What if the end user is different from the contract authority?

VENABLE LLP

Contract Administration

Manage Contract Changes:

- Provide Detailed Written Notice of Changes
  - Is unilateral change permitted?
  - Provide an early estimate of the cost impact so the CO understands potential liability
- Keep Written Records
  - Contemporaneous notes
  - Follow up email confirmations
  - Always keep the CO in the loop

VENABLE LLP

Contract Administration

Manage Contract Changes:

- Track Costs Associated with Change (*e.g.*, New Charge Number)
  - Timely request equitable adjustment *(e.g.,* 30-day limit under 52.243-1(c), 52.242-15(b)(2))
- Balance Spirit of Cooperation with Protecting Your Rights
  - Are you going to enforce every change?
  - Be careful about waiving certain rights, establishing a course of dealing that makes it more difficult to enforce rights later

The Civil False Claims Act

Overview

- The deepest pothole, for government contractors today, is the increasing rigidity of compliance enforcement.
- There is no question that the civil false claims statute was designed to target companies doing business with the government.
- The qui tam (aka Whistleblower) provision of the FCA is the most troublesome for companies doing business with the government. It is the primary source of litigation by the government for recovery from it. Of the $3.3 billion recovered in calendar year 2012, approximately 65% was based on the qui tam provision.

Overview

- There were approximately 730 FCA enforcement actions in 2012, two-thirds of which were brought by whistleblowers.
- 50% of the FCA cases deal with procurement fraud. These fraud cases come to the government's attention through: (i) the IG, (ii) mandatory disclosures, and (iii) whistleblowers.
- The vast majority of whistleblowers say that they went to the company first with no meaningful response.
- Of course, this fact indicates the need for companies to have robust compliance programs. If there's one key, it is undertaking meaningful training.

Civil False Claims Act

- The Civil False Claims Act provides penalties for any person who:
  - Knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval to an officer or employee of the United States government;
  - Knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim paid or approved by the government; or
  - Conspires to defraud the government by getting a false or fraudulent claim allowed or paid.

Civil False Claims Act (*cont.*)

- A "claim" is defined as:

  Any request or demand, whether under a contract or otherwise, for money or property that is presented to an officer, employee or agent of the United States, or is made to a contractor, grantee or other recipient, if the money or property is to be spent or used on the government's behalf or to advance a government program or interest and includes money or property of the government.

Civil False Claims Act (*cont.*)

- A claim is submitted "knowingly" when the claimant, with respect to the false information:
  - Has actual knowledge of the information;
  - Acts in deliberate ignorance of the truth or falsity of the information; or
  - Acts in reckless disregard of the truth or falsity of the information.
- Intent to defraud is NOT necessary under the FCA.
  - Deliberate ignorance
  - Reckless disregard
- An innocent mistake or mere negligence will not result in a violation of the FCA.

Problem Areas

- Sloppy/inaccurate time charging
- Failure to distinguish funds from different contracts at all times
- Inflated claims
- Counterfeit Parts

Penalties

- Civil penalty of between $5,500 and $11,000 per false claim; plus,
- Three times the amount of damages sustained by the government; as well as,
- The cost of any civil action brought to recover the penalties or damages.

Indicators of Fraud

- By Government Employees:
  - Excess purchases
  - SOWs written for a specific vendor
  - Improper sole-source justifications
  - Revealing information to specific contractors
  - Improper evaluation of offer/bids
  - Seemingly unnecessary contacts
  - Material changes in contract just after award
  - Backdating documents

Indicators of Fraud (*cont.*)

- By Employees:
  - Improper communications (*e.g.*, trade shows, professional meetings)
  - Improper social contact
  - Discussing possible employment after government service
  - Collusive bidding/price fixing
  - Cost mischarging

Indicators of Fraud (*cont.*)

- Cost Mischarging Examples:
  - Unallowable costs (political contributions, certain entertainment costs, advertising)
  - Labor mischarging (transfer of labor costs, timesheet fraud, ceiling limitations)
  - Commercial vs. government contracts
  - Material mischarging and product substitution

Other Red Flags of Fraud

- Lapses in the enforcement of the Code of Conduct or similar policy
- Transferring charges from one delivery order to another
- Unexpected resignation or replacement of key management personnel
- Managers retroactively assigning charge numbers
- Weakening in the company's financial condition (*e.g.*, recurring operating losses)
- Actual results not meeting forecasts

VENABLE LLP

Other Red Flags of Fraud (*cont*.)

- Unexpected year-end transactions that result in significant revenues
- Unusual accounting practices for revenue recognition and cost deferral
- Changes in accounting methods that are designed to enhance profit numbers
- Changes in independent accountants that resulted from disagreements

VENABLE LLP

Litigation: Minimizing Costs & Optimizing Opportunities for a Favorable Outcome

Litigation Risk

- Expect the unexpected!
- Develop policies that protect your company in the unlikely event that you will become involved in litigation.
  - Email policies
  - Document retention policies

Litigation Risk

- Email Policies:
  - Ensure that work emails are used for **WORK**
  - Stress importance of email etiquette
  - Keep email content limited to just the facts

Litigation Risk

- Document Retention:
  - How long will the documents be retained?
  - Can the documents be taken from the premises by an employee?
  - How will files/documents be processed when an employee leaves the company?

Litigation Risk

- Privileges:
  - Sensitize employees to protecting the attorney-client privilege.
  - Only use legends when appropriate.
  - Increased time and costs in conducting privilege reviews.
- Attorney-Client Privilege: "The client's right to refuse to disclose and to prevent any other person from disclosing confidential communications between the client and the attorney." Black's Law Dictionary (9th ed. 2009)
- Work Product: "Tangible material or its intangible equivalent — in unwritten or oral form — that was either prepared by or for a lawyer or prepared for litigation, either planned or in progress." Black's Law Dictionary (9th ed. 2009)

Litigation Risk

- What should you do when faced with possible litigation?
  - Preserve your evidence
  - Identify persons with knowledge of the issue
  - Establish structure or designate person to manage the litigation
  - Establish accounting codes so that the costs can be segregated
  - Select forum
- Spoliation

Litigation Risk

- What to do if you are involved in litigation?
  - Explore whether the litigation can be resolved through more informal means
  - Focus on getting the litigation resolved
  - Establish litigation goals and revisit every 4 to 6 months
  - Establish a budget
  - Continue to communicate with your customer
  - Don't forget the administrative causes of action

VENABLE LLP

Questions?

VENABLE LLP

Contact Information

YOUR VENABLE TEAM

Paul Debolt
padebolt@Venable.com
t 202.344.8384
f 202.344.8300

Bill Walsh
wlwalsh@Venable.com
t 703.760.1685
f 703.821.8949

James Boland
jyboland@Venable.com
t 703.760.1997
f 703.821.8949

www.Venable.com

Ethics and Compliance in a Heightened Enforcement Environment

1:00 p.m. – 2:00 p.m.

William Devaney, Venable LLP

Dismas Locaria, Venable LLP

Lindsay B. Meyer, Venable LLP

Susan Zoch, Merkle

VENABLE® LLP

VENABLE® LLP

Ethics and Compliance in a Heightened Enforcement Environment

April 10, 2014

VENABLE® LLP

Panelist Biographies

Lindsay B. Meyer, Venable LLP – Moderator

Lindsay Meyer is Co-Managing Partner of Venable and heads the International Trade Practice, assisting sophisticated companies to efficiently import and export under U.S. laws and regulations. As a licensed U.S. Customs broker, Ms. Meyer has a detailed knowledge of and extensive experience with the regulations of the U.S. Bureau of Customs and Border Protection. She is also co-chair of Venable's FCPA and Anticorruption Practice.

For over twenty years, Ms. Meyer has provided International Trade and Customs advice at Venable, where she heads Venable's International Practice based in Washington, DC. Ms. Meyer concentrates on all aspects of International Trade and Customs matters. She regularly advises companies on their compliance with import and export control laws and regulations, and appears before numerous regulatory authorities, such as the U.S. Customs and Border Protection (CBP), International Trade Commission (ITC), Commerce Department's Bureau of Industry and Security (BIS), State Department's Directorate of Defense Trade Controls (DDTC), Treasury Department's Office of Foreign Assets Control (OFAC), and the Committee on Foreign Investment in the United States (CFIUS).

Ms. Meyer has extensive experience counseling companies on compliance with export controls regulated by BIS, DDTC, and OFAC and actively assists companies in their registration and license authorization needs for exports, re-exports and deemed exports. She guides companies through internal Export Control Assessments, helps develop tailored compliance policies and procedures, and performs training on export laws and regulations affecting a company. Additionally, Ms. Meyer has successfully defended exporters facing civil and criminal investigations for alleged violations of U.S. export control laws and embargoes.

Ms. Meyer also advises clients on international transactional matters, where she counsels on strategic sourcing, targeted acquisitions Helms-Burton analysis, CFIUS investigations and FOCI reviews; sales and distribution arrangements in the U.S. and abroad; the use of foreign agents, affiliated offices, joint ventures and teaming agreements; as well as compliance with anti-boycott restrictions and anti-bribery laws, such as the U.S. Foreign Corrupt Practices Act (FCPA).

Panelist Biographies

Susan Zoch, Associate General Counsel, Merkle, Inc.

Currently Associate General Counsel at Merkle, Susan Zoch has enjoyed more than 14 years as in-house counsel in the marketing and advertising industry. Her experience in the industry includes domestic and international commercial transactions, licensing, employment, labor, real estate, privacy, safety and environmental compliance, and corporate matters.

Before going in-house, Ms. Zoch served as an Associate at Baker Botts, focusing on domestic and international transactional matters, and clerked for the U.S. District Court, Northern District of Texas. She earned her JD with honors at the University of Texas, where she served as Executive Editor of the *Texas Law Review*, and her BA at Rice University. Before law school, Ms. Zoch worked in software applications development at IBM.

Panelist Biographies

William (Widge) H. Devaney, Venable LLP

William (Widge) Devaney is co-chair of Venable's Foreign Corrupt Practices Act (FCPA) and Anti-Corruption Group. Mr. Devaney's practice includes white-collar criminal defense in federal and state proceedings, SEC enforcement investigations and actions, complex civil litigation, civil RICO, defending individuals and corporations in multi-national investigations, including FCPA and export control, as well as conducting national and international internal investigations on behalf of corporate management, audit committees and special committees of boards of directors.

Mr. Devaney has significant jury trial and appellate experience, as well as significant experience leading investigations. Mr. Devaney was an Assistant United States Attorney in the District of New Jersey, where he was most recently a member of the Securities Fraud Unit. As a federal prosecutor, Mr. Devaney investigated and prosecuted numerous cases involving securities fraud, bank fraud, mail and wire fraud, tax evasion, money laundering, terrorism, government program fraud, computer trespass, and export violations. Prior to joining the Department of Justice, Mr. Devaney practiced white-collar criminal defense and complex civil litigation, representing clients in federal and state criminal investigations, SEC and CFTC investigations, as well as attorney disciplinary proceedings.

VENABLE LLP

Panelist Biographies

Dismas (Diz) N. Locaria, Venable LLP

Dismas (Diz) Locaria is a member of the firm's Government Contracts Group. Mr. Locaria's practice focuses on assisting government contractors in all aspects of working with the federal government, as well as representing and counseling clients concerning the peculiarities of the Homeland Security Act's SAFETY Act.

Mr. Locaria has represented clients before various federal agencies, including the Department of Defense, General Services Administration, Department of Homeland Security, Small Business Administration, Environmental Protection Agency, and others. Mr. Locaria has developed several specialty areas, including representing clients in suspension and debarment proceedings, as well as performing internal investigations, which has included assistance and representation for such clients with disclosures to federal officials regarding the findings of such investigations and working with the client to determine and implement compliance enhancements and improvements. Mr. Locaria also has extensive experience in client counseling, including assisting clients with the nuances of becoming government contractors and implementing appropriate systems and methods to achieve and maintain regulatory and contractual compliance. Mr. Locaria is also well versed in assisting clients with GSA Federal Supply Schedule matters, in particular advising clients on how best to structure proposals to avoid price reduction clause (PRC) issues, and addressing PRC, Trade Agreements Act and other compliance matters post-award.

VENABLE LLP

Ethics and Compliance in a Heightened Enforcement Environment

- Events over the past 5 years
  - Federal debt and budget deficits
  - Tremendous expenditures related to wars in Afghanistan and Iraq
  - Economic downturn
- Made combatting contractor "waste, fraud and abuse" politically popular

Ethics and Compliance in a Heightened Enforcement Environment (cont'd)

- Increase in:
  - Congressional oversight
  - Agency audits
  - Reporting requirements – agency and contractor alike
  - Suspension and debarment activity
  - Public disclosure/transparency (e.g., FAPIIS)
  - Wider application of the Civil False Claims Act

Traditional Ethical Topics

- Export controls (ITAR, EAR, OFAC)
- False Statements Act/Criminal and Civil False Claims Acts
- Bribes, gifts and gratuities (*e.g.*, FCPA)
- The Anti-Kickback Act
- Lobbying and pay-to-play rules
- Organizational & Personal Conflicts of Interest
- Procurement Integrity Act
- Small business issues (*e.g.*, certification, teaming, etc.)
- Handling of confidential information
- Recruiting and soliciting employment to government officials
- Time card/labor hour records

VENABLE LLP

U.S. Export Controls: Practical Compliance Traps and Tips for Contractors

VENABLE LLP

Why Should Government Contractors Care?

- Do you work with detailed or sensitive information about U.S. products, software, or technology?
  - *e.g., aircraft parts, chemical agents, satellite systems*
- Do you interact with U.S. persons located overseas?
  - *e.g., contractors, multinational corporations, international organizations*
- Do you interact or collaborate by email with foreign persons either here or abroad?
  - *e.g., foreign agencies, state-controlled entities, visiting researchers*
- Do you travel outside the U.S. with a computer or documents containing work-related information?
  - *e.g., overseas international consortium, research presentations*

Primary Regulatory Agencies

- Export Control Laws and Regulations
  - International Traffic in Arms Regulations (ITAR)
    - Defense articles
    - Administered by State Dep't, DDTC
  - Department of Defense Regulations (DoD)
    - Defense items
    - Classified (NISPOM) and unclassified articles
  - Export Administration Regulations (EAR)
    - Dual-Use Items
    - Administered by Commerce Dep't, BIS
  - Office of Foreign Assets Control (OFAC) Regulations
    - US sanctions program
    - Administered by Dep't of Treasury, OFAC

Who Is Affected?

- Are you dealing with the following?
  - Persons:
    - All U.S. "persons," wherever located
    - All persons in the U.S., regardless of nationality
  - Governments
    - Focus on State-controlled entities
    - Governmental End-Use
  - Countries
    - Borders matter
    - Jurisdiction attaches

Compliance Considerations

- Do you understand the recent changes from the Administration's Export Control Reform?
- Do you follow DFARs 252.204-7008 flowdown provisions?
- Are you complying with I-129 Form U.S. Export Control Certification for Visa Applications?
- Have you kept current with subcontractor changes on TAAs and MLAs?
- Do you follow all conditions of issued licenses? (quantity; value; end-users)
- Failure to do so → significant fines & penalties

Compliance Traps for Contractors

- Export Authorization Controls:
  - Over-shipped quantity/value
  - Unauthorized transfers in country
  - "DoD Approval" or direction ≠ license
  - Failure to get USG authorization for license exception
  - Forgetting flowdown provisions
    - DFARs 252.204-7008
    - 67 Fed. Reg. 18,029 (Apr. 10, 2010)
- Tip: Train to Manage this Function

More Compliance Traps for Contractors

- Reexport Authorization Controls:
  - Different intermediate consignee
  - Different end-user organization
- Unauthorized Transfers in Country
  - Different intermediate consignee
  - Different end-user
- Post Project "Cleanup"
  - Close out licenses and return of goods
  - Import license needed? Goods left behind?
- Tip: Can't "outsource" responsibility, follow-up

Ubiquitous Controlled "Defense Services"

- Defense Services Occur More Often Than Realized
  - Clarification on dealing with non-ITAR items
  - Who exactly are you dealing with?
  - Are your services "training"?
  - Complex organizational structures with foreign defense oversight
- When in Doubt, Inquire:
  - CJ requests to confirm/clarify
- Tip: Due Diligence on all Parties to the Transaction: Check Upstream Control

Deemed Export Difficulties

- Managing your (or the USG's) Technology?
  - Maintaining a current "inventory"
  - Marking and managing same?
- Lack of In-house Worker "Inventory"
  - Visa ≠ export license
    - Spouse visa not sufficient
    - Manage green card validity periods
  - Remember Immigration Form I-129
    - Applicants for H-1B, H-1B1, L-1 or O-1A
    - Burden on company to certify (Feb. 2011)
    - False statement charge?
- Flowdown to Subs? Or Service Providers?
- Tip: Include Contractual Provisions

Consider Other Authorizations

- Sloppy Agreement Management
  - Ever-changing subs on TAAs & MLAs
  - Lack of control on nationalities (3rd country?)
  - Failure to follow conditions
  - Changing facts with lack of authorization updates
- Distribution Agreements
  - Lack of controls downstream
  - Failure to follow up
- Tip: Centralize Control - Legal Oversight / Privilege

Tiptoe Carefully Through US Economic Sanctions and Embargoes

- National Security Basis for Prohibitions and Restrictions
  - Ever-changing targets and policies
  - Regulations "similar" but not Identical
  - Multiple lists now consolidated
    - Fail to follow debarred parties, denial orders
  - Consider other sanction programs' impact
    - UN sanctions, EU sanctions, etc.
    - Often in tandem with U.S. license authorization, but not identical
- Tip: Automate List Review to Meet Business Operations

Why Do We Care? Penalties, and Not Just Monetary Ones

- Criminal Penalties
  - $1,000,000 per violation and/or
  - 20 years imprisonment for individuals
  - Prosecution by Department of Justice
- Civil Administrative Penalties
  - Fines up to $250,000 per violation or twice the amount of the transaction at issue, whichever is greater and/or
  - Placement on debarred parties, denied persons list, SDN list
  - Don't kill the golden goose!

Review of Recent Cases and Settlements Demonstrate Trends

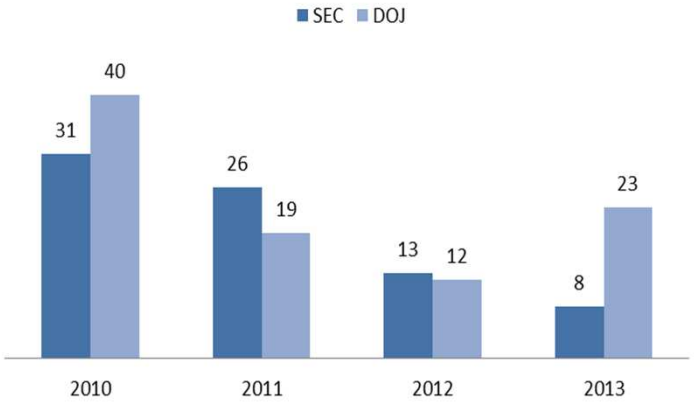
- Trends:
  - Significant fines
  - Focus on individuals along with organizations
  - Coordinated investigations
    - Across agencies (State, BIS, OFAC)
    - Types of violations (FCPA, anticorruption, etc.)
  - Outside monitoring and independent audits
  - Disclosures continue
    - Increasing with whistleblower cases?
  - Proactive compliance is critical
    - Undertake before an investigation
    - Training and monitoring imperative
    - Support of upper management

FCPA 2013:

Facts and Figures

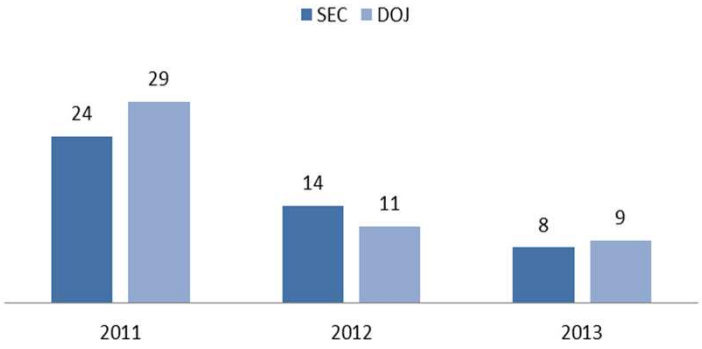
VENABLE LLP

Total SEC/DOJ Enforcement Actions by Year

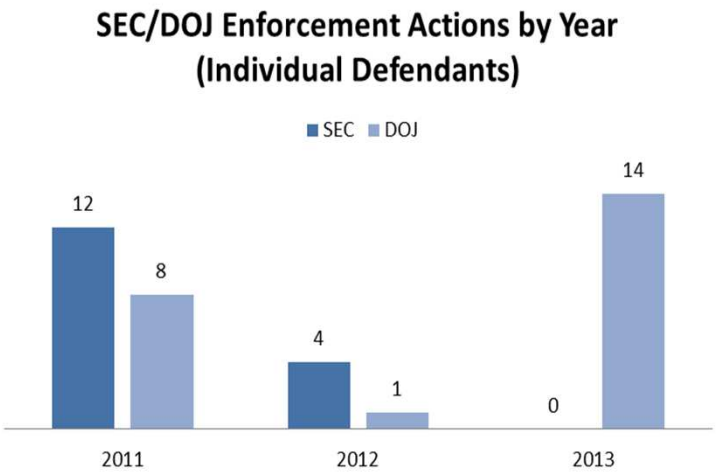


VENABLE LLP

SEC/DOJ Enforcement Actions by Year (Corporate Defendants)



VENABLE LLP



VENABLE LLP

Fines and Penalties

- In 2013, DOJ and the SEC combined imposed more than $720 million in penalties – more than double the value of penalties imposed overall in 2012.
- This figure includes the penalties imposed against French oil and gas company Total, S.A. (DOJ: $245.2 million; SEC: $152.8 million), and Weatherford International, Ltd. (DOJ: $86.8 million; SEC: $65.6 million) – the fourth largest and ninth largest FCPA enforcement actions ever.

VENABLE LLP

2013 Corporate Penalties

BILFINGER
($32 million)

TOTAL
($398 million)

ADM
($44.8 million)

PARKER DRILLING
($15.85 million)

stryker
($13. million)

Weatherford
($152 million)

PHILIPS
($4.5 million)

DIEBOLD
INNOVATION DELIVERED
($48.17 million)

RALPH LAUREN
($1.6 million)

VENABLE LLP

Enforcement Against Individuals

- **In 2013...**
  - **Paul Novak,** sentenced to 15 months in prison and forced to pay a $1 million criminal fine for his involvement in the *Willbros* case.
  - **Neal Uhl**, sentenced to 5 years on probation and 8 months home confinement for his involvement with the *Bizjet* case.
  - **Peter DuBois**, sentenced to 5 years on probation and 8 months home confinement for his involvement with the *Bizjet* case.
  - Additional 6 people **charged**, 5 people **pleaded guilty** and await sentencing
- **In 2012…**
  - **Jean Rene Duperval**, sentenced to 9 years in prison for his involvement in the *Haiti Telecom* case. Duperval is the first foreign official to stand trial in connection with an FCPA case.
  - **Albert Jack Stanley**, sentenced to 30 months in prison for his involvement in the *KBR/TSKJ* case.
  - **Manuel Caceres**, sentenced to 23 months in prison for his involvement in the *Latin Node* case.
  - **Fernando Basurto**, sentenced to time served after spending 22 months in prison for his involvement in the *ABB* case.
  - **Jeffrey Tesler**, sentenced to 21 months in prison for his involvement in the *KBR/TSKJ* case.

VENABLE LLP

2013 Trends

- Continued prosecution of individuals - The DOJ announced charges against 14 individuals, more than any year since 2010
- International cooperation - International anti-corruption enforcement continues to grow, and several foreign law enforcement agencies assisted in U.S. investigations in 2013.
- Foreign defendants - The SEC and DOJ continued to prosecute foreign defendants; approximately 9 defendants were non-U.S.-based.
- Industry Trends: oil & gas; aviation; energy; financial services; and life sciences

VENABLE LLP

False Claims Act

False Claims Act - 31 U.S.C. § 3729-33

(a) Liability for Certain Acts. —

(1) In general.— Subject to paragraph (2), any person who-

(A) knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval;
(B) knowingly makes, uses, or causes to be made or used a false record or statement material to a false or fraudulent claim;
(C) conspires to commit a violation of subparagraph (A), (B), (D), (E), (F), or (G);
(D) has possession, custody, or control of property or money used, or to be used, by the Government and knowingly delivers, or causes to be delivered, less than all of that money or property;
(E) is authorized to make or deliver a document certifying receipt of property used, or to be used, by the Government and, intending to defraud the Government, makes or delivers the receipt without completely knowing that the information on the receipt is true;
(F) knowingly buys, or receives as a pledge of an obligation or debt, public property from an officer or employee of the Government, or a member of the Armed Forces, who lawfully may not sell or pledge property; or
(G) knowingly makes, uses, or causes to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the Government, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the Government, is liable to the United States Government for a civil penalty of not less than $5,000 and not more than $10,000, as adjusted by the Federal Civil Penalties Inflation. Adjustment Act of 1990 (28 U.S.C. 2461 note; Public Law 104-410), plus 3 times the amount of damages which the Government sustains because of the act of that person.

False Claims Act

(b) Definitions.— For purposes of this section—

(1) the terms "knowing" and "knowingly"—

(A) mean that a person, with respect to information—

(i) has actual knowledge of the information;

(ii) acts in deliberate ignorance of the truth or falsity of the information; or

(iii) acts in reckless disregard of the truth or falsity of the information; and

(B) require no proof of specific intent to defraud;

(2) the term "claim"—

(A) means any request or demand, whether under a contract or otherwise, for money or property and whether or not the United States has title to the money or property, that—

(i) is presented to an officer, employee, or agent of the United States; or

(ii) is made to a contractor, grantee, or other recipient, if the money or property is to be spent or used on the Government's behalf or to advance a Government program or interest, and if the United States Government—

(I) provides or has provided any portion of the money or property requested or demanded; or

(II) will reimburse such contractor, grantee, or other recipient for any portion of the money or property which is requested or demanded; and

(B) does not include requests or demands for money or property that the Government has paid to an individual as compensation for Federal employment or as an income subsidy with no restrictions on that individual's use of the money or property;

(3) the term "obligation" means an established duty, whether or not fixed, arising from an express or implied contractual, grantor-grantee, or licensor-licensee relationship, from a fee-based or similar relationship, from statute or regulation, or from the retention of any overpayment; and

(4) the term "material" means having a natural tendency to influence, or be capable of influencing, the payment or receipt of money or property.

False Claims Act

1. **Factually false claims** – Goods and services are billed for, but never provided
2. **Legally false claims** – when a claim fails to satisfy an underlying legal requirement because of a violation of a statute, regulation, or contract. The underlying violation can become actionable under the FCA through a certification, which can take one of two forms:
    1. *Express certification* – the claim submitted affirmatively certified compliance with the underlying law
    2. *Implied certification* – the party submitting the claim violated an ongoing obligation to comply with a statute, regulation, or contract, but did not affirmatively certify compliance in its claim submission
        - As explained by the Ninth Circuit Court of Appeals:

"Implied false certification occurs when an entity has ***previously undertaken to expressly comply*** with a law, rule, or regulation, and that obligation is implicated by submitting a claim for payment even though a certification of compliance is not required in the process of submitting the claim." *Ebeid ex rel. United States v. Lungwitz*, 616 F.3d 993, 998 (9th Cir. 2010), cert. denied, 131 S.Ct. 801 (2010)

Different Readings: "Implied Certification"

- Second, Third, Sixth, Ninth, and Tenth Circuits:
  - To be false, a claim must violate a law that was an express condition to payment
    - *Mikes v. Straus,* 274 F.3d 687 (2d Cir. 2001)
    - *United States ex rel. Wilkins v. United Health Group, Inc.*, No. 10-2747, 2011 WL 2573380 (3rd Cir. June 30, 2011)
    - *United States ex rel. Chesbrough v. VPA, P.C. dba Visiting Physicians Ass'n*, No. 10-1494, 2011 WL 3667648 (6th Cir. Aug 23, 2011)
    - *Ebeid ex rel. United States v. Lungwitz,* 616 F.3d 993 (9th Cir. 2010), *cert. denied*, 131 S.Ct. 801 (2010)
    - *United States ex rel. Conner v. Salina Reg. Health Ctr., Inc.*, 543 F.3d 1211 (10th Cir. 2008)
- Eleventh and D.C. Circuits (more expansive view):
  - To be false, the law violated does not have to be a prerequisite for payment
    - *McNutt ex rel. United States v. Haleyville Med. Supplies, Inc.,* 423 F.3d 1256 (11th Cir. 2005)
    - *United States v. Sci. Apps. Int'l Corp.*, 626 F.3d 1257 (D.C. Cir. 2010)
- First Circuit:
  - To be false, a claim must misrepresent compliance with a law that was a material precondition to payment
    - *United States. ex rel. Hutcheson v. Blackstone Med., Inc.*, 647 F.3d 377 (1st Cir. 2011)

False Claims Act – FY 2013 Statistics

- Approximately $3.8 billion recovered by the federal government under the False Claims Act
- More than 846 new cases filed under the FCA
  - 752 (89%) of cases were filed by *qui tam* "Relators"
    - Relators earned more than $387 million in share awards
      - The government ultimately intervenes in approximately 20% of *qui tam* matters

False Claims Act – FY 2013 Statistics

- Industry Breakdown
  - Healthcare/Life Sciences:
    - $2.6 billion
  - Defense/Procurement:
    - $887 million
  - Non Healthcare/Defense:
    - $612 million

VENABLE LLP

Dodd-Frank Act – FY 2013 Statistics

- Additional risk for publicly traded government contractors:
  - **During fiscal year 2013, the SEC received 3,238 tips (an 8% increase from 2012)**
    - Received tips from all 50 U.S. states, D.C., Puerto Rico, Guam, and the U.S. Virgin Islands
    - Received tips from 55 foreign countries
  - **Made more than $14 million in award payments to whistleblowers**
  - **Most common submissions:**
    - Corporate disclosures and financials – 557 tips
    - Offering fraud – 553 tips
    - Manipulation – 525 tips
    - Other categories include: "Insider Trading," "Trading and Pricing," "FCPA," "Unregistered Offerings," "Market Event," "Municipal Securities and Public Pension," and "Other"

VENABLE LLP

Avoiding Ethical Pitfalls & Enforcement Actions

VENABLE LLP

Basic Ethical Rules and Obligations – The Basics

- Exercise the highest degree of honesty and integrity in dealings with others.
- Conduct your business in accordance with the law and in an ethical manner.
- Avoid practices that may create even the ***appearance*** of impropriety.
- Know or learn the rules and requirements of your government contracts.
- Do not rely on a government employee's representation regarding the applicable rule or requirement (no matter who the government employee is).
- If you are unsure how to proceed, do not hesitate to ask for guidance.
- Promptly report suspected violations to management.

VENABLE LLP

Sobering Statistics – GSA OIG

Department of Defense (Oct. 1, 2012-Mar. 31, 2013)	General Services Administration (FY 2013)
Identified $1.3B in potential monetary benefits	Over $1.7B in recommendations that funds be put to better use/ questioned costs
$1.6B returned to the USG	$253M in criminal, civil, administrative, and other recoveries
56 arrests, 102 criminal charges, 98 criminal convictions	80 criminal indictments/informations and 56 successful prosecutions on criminal matters referred
98 suspensions and 95 debarments	172 contractor/individual suspensions and 194 contractor/individual debarments

VENABLE LLP

Creating an Environment That Fosters Ethical Conduct

- Culture of compliance
- Integrated into all facets of your operation
- Five elements of compliance

Compliance Elements	Examples
Policies & Procedures	• Code of conduct • Compliance program
Systems & Tools	• Business systems • Internal hotline
Training & Communications	• Statement from top management • Ethics training
Organizational Considerations	• Appointment of a compliance officer
Oversight & Monitoring	• Internal audit function

VENABLE LLP

Creating an Environment that Fosters Ethical Conduct (cont'd)

- Code of Conduct
  - Required under the FAR for all contractors
  - Requires:
    - Code to be provided to all employees
    - Due diligence to prevent and detect criminal conduct
    - Promotion of a culture of compliance
- Compliance Program
  - Required for "other than small" contractors
  - Requires:
    - Appointment of a compliance officer
    - Periodic communication of the program to employees
    - Compliance training
    - Periodic review of compliance policies and procedures
    - Compliance reporting mechanism
    - Discipline for unethical/noncompliant conduct
    - Disclosure for ethical noncompliance and "substantial" overcharges

Investigating Ethical Concerns

- Internal reporting channels
  - Obligations to establish reporting channels
    - Sarbanes-Oxley (SOX)
    - Federal Acquisition Regulation (FAR)
    - Others
  - Handling internal reports
    - Investigate?
      - Required – SOX, FAR
      - Incentivized – SEC, FINRA, DOJ guidelines
    - Anti-retaliation
    - Confidentiality

Investigating Ethical Concerns (cont'd)

- Considerations
  - Stop suspected conduct
  - Avoid conflicts of interest
    - Who will "control" the investigation
    - Use of outside counsel
  - Maintain "privilege" and confidentiality
  - Scope of investigation
    - Goal of investigation
    - Topic(s)
    - Documents
    - Interviews
  - Written findings
  - What will be done with the results
  - Disputes/appeals

Investigating Ethical Concerns (cont'd)

- Best Practices
  - Clear and objective owner of investigation
  - Investigator must also be objective
  - Clearly define scope of investigation
  - Develop an investigation plan
  - Be willing to revisit plan and change course
  - Stop continuing misconduct
  - Preserve all potentially relevant documents (including emails)
  - Be prepared before interviewing employees
  - *Upjohn* warnings
  - Anti-retaliation policy
  - Confidentiality
  - Examine corrective measures

Reporting Requirements

- Mandatory disclosures
  - FAR
    - Credible evidence of a significant overpayment, civil false claim, federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations
    - Cognizant IG's office and contracting officer
  - SOX
    - Material changes in the financial condition or operation of the company
    - SEC filings
  - Super Circular – applies to grant funds
    - Standard similar to that of FAR

VENABLE LLP

Questions?

Lindsay B. Meyer
202.344.4829
LBMeyer@Venable.com

Susan Zoch
443.542.4662
szoch@merkleinc.com

William (Widge) H. Devaney
212.983.8204
WHDevaney@Venable.com

Dismas (Diz) Locaria
202.344.8013
DLocaria@Venable.com

Cyber Pros and Cons for Government Contractors

2:10 p.m. – 3:00 p.m.

Keir X. Bancroft, Venable LLP

Jamie Barnett, Venable LLP

Scott Hommer, Venable LLP

Kimberly deCastro, Wildflower

Jim Winner, Northrop Grumman Corporation

Jason R. Wool, Venable LLP

VENABLE® LLP

VENABLE® LLP

Cyber Pros and Cons for Government Contractors

APRIL 10, 2014

VENABLE® LLP

J. Scott Hommer, III – Moderator

Venable LLP

Scott Hommer serves as a partner in the Tysons Corner office of Venable LLP. He concentrates his practice in business counseling and litigation, with an emphasis on technology companies and government contractors. He represents clients locally, nationally, and internationally on issues including negotiating contracts, doing acquisitions, protecting intellectual property rights, and litigating successfully. Mr. Hommer also has significant experience in counseling clients who do business with the federal, state, and local governments and has represented clients on contract administration matters, contract claims and disputes, bid protests, contract terminations, teaming agreements, conflicts of interest issues, intellectual property rights issues, government socio-economic programs, and small business matters.

Mr. Hommer is committed to developing relationships with his clients that go beyond the usual role of legal advisor. He works closely with his clients on a proactive basis, developing strategic plans and managing legal issues that may arise, and, more importantly, identifying potential problems before they develop. This approach is not only smart; it is efficient and cost-effective and significantly enhances opportunities for success.

VENABLE LLP

Jim Winner

Assistant General Counsel, Northrop Grumman Corporation

Jim Winner is lead counsel for Northrop Grumman's Cyber Solutions Division. Prior to joining Northrop Grumman, Jim served in legal and contracts leadership roles for ITT Corporation, including Vice President and General Counsel and Vice President, Contracts and Procurement for ITT Information Systems (Herndon, VA) and Associate General Counsel for ITT Mission Systems (Colorado Springs, CO). Jim also practiced law with Barnes & Thornburg LLP (Indianapolis, IN), specializing in contracts, procurement , and labor and employment law, and worked in-house for Rolls-Royce Corporation and Cummins Inc.

Prior to joining the private sector, Jim honorably served as an Air Force judge advocate and systems acquisition officer. In the Air Force, Jim worked across multiple legal disciplines, including trial and appellate litigation, and served as a non-lawyer acquisition professional in the Military Satellite Communications (MILSATCOM) Joint Program Office, where he supported major satellite communications programs, including DSCS, Milstar and Advanced EHF.

VENABLE LLP

Jamie Barnett, Rear Admiral (Ret.)

Venable LLP

Admiral Barnett is Co-Chair of Venable's Telecommunications Group and a partner in the firm's Cybersecurity Practice. He has a rare combination of experience in cybersecurity, national defense, homeland security, emergency communications, public safety communications and technology policy. This experience is invaluable to clients in the financial services, transportation, telecommunications and utilities industries as well as other critical infrastructures.

Admiral Barnett has had a distinguished career in the public and private sector. A surface warfare officer, he has over 30 years of experience in the United States Navy and Navy Reserve, rising to the rank of Rear Admiral and serving as Deputy Commander, Navy Expeditionary Combat Command and Director of Naval Education and Training in the Pentagon. Among other personal awards, he has received four Legion of Merit medals.

In addition to his military service, Admiral Barnett served as the Chief of the Public Safety and Homeland Security Bureau of the Federal Communications Commission where he executed major cybersecurity initiatives. As Chief of the Bureau, Admiral Barnett also led major rulemakings and projects in public safety broadband, emergency alerting and Next Generation 9-1-1, working closely with industry and government stakeholders. He has also testified before Congress and is a noted speaker on cybersecurity.

VENABLE LLP

Keir X. Bancroft

Venable LLP

Keir Bancroft provides a range of services to government contractors. Mr. Bancroft represents clients in litigation, including bid protests, size and status protests, and contract-related disputes before tribunals including the GAO, the SBA, boards of contract appeal and the United States Court of Federal Claims.

Mr. Bancroft also drafts and negotiates subcontracts, nondisclosure agreements, joint ventures, mentor-protégé agreements, and licensing agreements on behalf of clients.

Within the broad rubric of cybersecurity, Mr. Bancroft specializes in information security and privacy compliance. He helps clients comply with standards under the Federal Information Security Act (FISMA), the Department of Defense Information Assurance guidelines, the Privacy Act, and similar requirements. Mr. Bancroft also focuses on national security and industrial security issues arising under the National Industrial Security Program Operating Manual (NISPOM).

Before joining private practice, Mr. Bancroft served as an attorney advisor and the Privacy Officer in the United States Department of the Treasury, Bureau of Engraving and Printing. There, he counseled and represented the Bureau in all facets of federal procurement and was responsible for ensuring Bureau systems complied with privacy and information security requirements.

VENABLE LLP

Jason R. Wool

Venable LLP

Jason Wool is an experienced cybersecurity attorney who specializes in advising clients on the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards. He has also contributed to the development of cybersecurity regulation and policy, including the Cybersecurity Framework developed by the National Institute of Standards and Technology under the auspices of Executive Order 13636. Mr. Wool also specializes in electric and other utility regulation at the state and federal levels. He has specifically focused much of his career on advising ISOs and RTOs on reliability compliance as well as a variety of other issues before the Federal Energy Regulatory Commission (FERC).

VENABLE LLP

Agenda

- Current cybersecurity requirements
- Cybersecurity Framework
- Practical implications and industry response
- Considerations for thriving in cybersecurity

VENABLE LLP

Current Cyber Requirements

DFARS Rule on Safeguarding Unclassified Controlled Technical Information

- Applies to unclassified controlled technical information resident on or transiting through contractor's unclassified information systems.
  - Definition: "technical data or computer software with military or space application that the Department has marked as controlled in accordance with DoD Instruction 5230.24 – Distribution Statements on Technical Documents."

Current Cyber Requirements

DFARS Rule on Safeguarding Unclassified Controlled Technical Information

- Contractor must demonstrate "adequate security" using the following options:
  - Apply specific NIST SP 800-53 security controls;
  - Demonstrate certain 800-53 controls are inapplicable; or
  - Demonstrate alternative and equivalent security measures. . .
  - . . . Or additional measures if the contractor determines necessary.

Current Cyber Requirements

DFARS Rule on Safeguarding Unclassified Controlled Technical Information

- Cyber Incident Reporting Obligations
  - Must report cyber incident resulting in "actual or potentially adverse" effect on information/information systems.
  - Report within 72 hours.
  - Include detailed damage assessment report.
  - Must preserve images of affected systems for 90 days.
  - Applies to subcontractors and outsourced IT infrastructure (*e.g.*, ISPs and cloud service providers).

Current Cyber Requirements

DFARS Rule on Safeguarding Unclassified Controlled Technical Information

- Assessing Compliance
  - Contracting Officer, with "security manager," will assess compliance.
  - Contracting Officer may audit and review contract compliance.
  - Report is not an indicator, in itself, of a failure to comply.
  - Conversely, report is not considered to be a safe harbor statement.

Current Cyber Requirements

2013 National Defense Authorization Act

- Section 941
  - Mandatory reporting for "cleared defense contractors" with authorization to access, receive, store classified information.
  - Required procedures from DoD for reporting when network or information system "successfully penetrated."
  - Must provide DoD personnel access to conduct forensic analysis.

VENABLE LLP

Emerging Cyber Requirements
What They Mean For Your Business

- Section 8(e) Recommendations
  - *Coordinated by DoD and GSA Joint Working Group*
- Presidential Policy Directive ("PPD") 21

VENABLE LLP

Cybersecurity Executive Order 13636
Acquisition Recommendations Per Sec. 8(e)

- DoD and GSA Joint Working Group
- Recommendations to the President on:
  - Feasibility,
  - Security benefits, and
  - Relative merits of incorporating security standards into acquisition planning and contract administration.

VENABLE LLP

Cybersecurity Executive Order 13636
Definition of "Cybersecurity"

- Broad definition of "cybersecurity," including:
  - Information security
  - Supply chain risk management,
  - Information assurance,
  - Software assurance,
  - As well as other efforts to address threats or vulnerabilities flowing from or enabled by connection to digital infrastructure.

VENABLE LLP

Cybersecurity Executive Order 13636
Acquisition Recommendations Per Sec. 8(e)

- Recommendations (released January 23, 2014)

1. Institute Baseline Cybersecurity Requirements as a Condition of Contract Award for Appropriate Acquisitions.
   - Updated virus protections, multiple factor logical access, data confidentiality, current security software patches.
   - Include in technical requirements for acquisitions, and include performance measures to 1) ensure baseline is maintained, and 2) risks are identified throughout the lifespan of the product or service acquired.

Cybersecurity Executive Order 13636
Acquisition Recommendations Per Sec. 8(e)

2. Address Cybersecurity in Relevant Training.
   - Acquisition cybersecurity outreach campaign targeted at industry stakeholders.
     - GSA "Pathway to Success," a mandatory training program for would-be schedule offerors, training cited as an example.
   - Clarify the government is changing buying behavior relative to cybersecurity by adopting a risk-based methodology.
   - More will be required from industry relative to cybersecurity in certain acquisitions.

Cybersecurity Executive Order 13636
Acquisition Recommendations Per Sec. 8(e)

3. Develop Common Cybersecurity Definitions for Federal Acquisitions.
   - Refers to "consensus based, international standards" as a baseline for common definitions.
   - Expressly seeks to harmonize the recommendation with DFARS rulemaking, "Detection and Avoidance of Counterfeit Electronic Parts."

Cybersecurity Executive Order 13636
Acquisition Recommendations Per Sec. 8(e)

4. Institute a Federal Acquisition Cyber Risk Management Strategy.
   - Recommends aligning strategy with the procedures developed in the Cybersecurity Framework.
   - Recommends "Overlays," or sets of security requirements (and guidance) to tailor security requirements for technologies or product groups, circumstances, conditions, and/or operational environments.
   - Overlays should be applied as technical requirements to acquisitions.

Cybersecurity Executive Order 13636
Acquisition Recommendations Per Sec. 8(e)

5. Include a requirement to purchase from original equipment manufacturers, their authorized resellers, or other "trusted" sources, whenever available, in appropriate acquisitions.
   - Risk mitigation might require obtaining items from OEMs, authorized resellers, or other trusted sources.
     - Recent draft RFP for NASA SEWP contract includes limitation of sources for certain types of items.

VENABLE LLP

Cybersecurity Executive Order 13636
Acquisition Recommendations Per Sec. 8(e)

5. OEM/Trusted Sources (continued)
   - Trusted sources – may be identified through use of qualified bidders, or manufacturers lists (QBLs).
     - Standards derive from level of cyber risk mitigation.
   - Non-OEMs or trusted sources must guarantee the security and integrity of an item being purchased.
   - For high cyber-risk procurements, government audit may be necessary to evaluate qualifications to provide items.

VENABLE LLP

Cybersecurity Executive Order 13636
Acquisition Recommendations Per Sec. 8(e)

6. Increase Government Accountability for Cyber Risk Management.
   - Requires key government decision makers to be held accountable for decisions regarding threats, vulnerabilities, likelihood and consequences of cybersecurity risks in a fielded solution.
   - Cyber risk management plan must be developed and overlays applied.
   - Acquisition personnel must certify appropriate cybersecurity requirements are adequately reflected in the solicitation.

VENABLE LLP

Cybersecurity Executive Order 13636
Acquisition Recommendations Per Sec. 8(e)

6. Government Accountability (continued)
   - During source selection, acquisition personnel must ensure apparent best value proposal meets cybersecurity requirements.
   - Post-award conformance testing: program executive must certify the activity conducted in accordance with prescribed standards.

VENABLE LLP

Cybersecurity Executive Order 13636
Draft Implementation Plan Per Sec. 8(e)

- Implements Recommendation 4: *Institute a Federal Acquisition Cyber Risk Management Strategy*
  - Aims to develop a repeatable, scalable process to address cyber risk in federal acquisition, based on risk inherent in the product or service.

VENABLE LLP

Cybersecurity Executive Order 13636
Draft Implementation Plan Per Sec. 8(e)

- Process:
  - Government will group Acquisitions presenting cyber risk into "Categories."
  - Risks "prioritized" based on comparative assessment in a Category.
  - Government will assign resources and develop "Overlays," including risk mitigations based in procurement and information security packages. (e.g., NIST SP 800-53 security controls, source selection criteria, pricing methodologies, contract performance indicators, etc.).

VENABLE LLP

Cybersecurity Executive Order 13636
Draft Implementation Plan Per Sec. 8(e)

- First Tasks to Undertake:
  1. Develop acquisition categories (includes establishing a taxonomy and conducting a spend analysis).
  2. Acquisition risk assessment and prioritization.
  3. Develop methodology to create Overlays (determine appropriate security controls, acquisition mitigations, other safeguards).

VENABLE LLP

Cybersecurity Executive Order 13636

Draft Implementation Plan Per Sec. 8(e)

- Joint Working Group Request for Comments:
  - Request for public comment on:
    - 6 Recommendations.
    - Draft Implementation Plan.

Public Comments Due April 28, 2014

VENABLE LLP

16 Critical Infrastructure Sectors

Definition of "Critical Infrastructure"

- Critical Infrastructure:
  - systems and assets,
  - whether physical or virtual,
  - so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on
  - **security,**
  - **national economic security,**
  - **national public health or safety,**
  - or any combination of those matters.

USA PATRIOT Act, 42 U.S.C. Sec. 5195c(e)

VENABLE LLP

16 Critical Infrastructure Sectors
By Sector-Specific Agency

- Covers a broad range of industries, and multiple agencies:
- DHS
  1. Chemical
  2. Commercial Facilities
  3. Communications
  4. Critical Manufacturing
  5. Dams
  6. Emergency Services
  7. Information Technology
  8. Nuclear Reactors, Materials, and Waste

VENABLE LLP

16 Critical Infrastructure Sectors
By Sector-Specific Agency

- DHS/GSA
  9. Government Facilities
- DHS/DOT
  10. Transportation Systems
- DOD
  11. Defense Industrial Base
- DOE
  12. Energy
- Treasury
  13. Financial Services

16 Critical Infrastructure Sectors
By Sector-Specific Agency

- HHS
  14. Healthcare and Public Health
- HHS/USDA
  15. Food and Agriculture
- EPA
  16. Water and Wastewater Systems

Presidential Policy Directive 21
National Policy on Security and Resilience

- Three Strategies:
  - Refine and clarify functional relationships across government.
  - Enable efficient information exchange by **identifying baseline data and systems requirements** for the federal government.
  - Implement an integration and analysis function to inform planning and operational decisions.
    - Shall use information and intelligence from states, local entities, **and nongovernmental analytic entities.**

VENABLE LLP

Presidential Policy Directive 21
National Policy on Security and Resilience

- Preview of "Identifying Baseline Data and Systems Requirements":
  - Proposed FAR rule on requiring basic safeguards for government contractor information systems.
    - **Restrict information** on public computers or Web sites without access control.
    - **Protect electronic information transmissions.**
    - **Apply Physical and electronic security.**
    - **Protect against intrusion** by applying anti-virus software and anti-spyware and promptly applying patches, service packs, and hot fixes.

VENABLE LLP

Presidential Policy Directive 21
Acquisition-Related Requirements

- Requires DoD, DHS, and GSA to provide and support government-wide contracts for critical infrastructure systems and **ensure inclusion of audit rights for security and resilience of critical infrastructure.**

VENABLE LLP

Presidential Policy Directive 21

Requires Aligning Federal R&D Activities

- Promote R&D for secure and resilient **design and construction of critical infrastructure**, and **accompanying technology.**
- Invest in **modeling capabilities** to determine impacts on critical infrastructure (and other sectors) of an incident or threat scenario (*i.e.*, Big Data).
- **Incentivize cybersecurity investments and adoption of design features** strengthening all-hazards security and resilience.

VENABLE LLP

EO 13636

Improving Critical Infrastructure Cybersecurity

- Directs NIST to develop a Cybersecurity Framework "to reduce cyber risks to critical infrastructure." § 7(a)
- Directs DHS to establish a voluntary program to support adoption of the Framework by owners and operators of Critical Infrastructure. § 8(a)
- Directs DHS to coordinate establishment of a set of incentives to promote participation in this program. § 8(d)

EO 13636 (continued)

Improving Critical Infrastructure Cybersecurity

- Required DoD and GSA to make recommendations to President regarding "feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration." § 8(e)
- Recommendations issued January 23.
- For acquisitions that pose cyber risks, recommends requiring government to do business only with organizations that meet baseline cybersecurity hygiene requirements in their operations and in the products and services they deliver.

Cybersecurity Framework

Where We Are

- Final Framework (version 1.0) was issued February 12, 2014.
- DHS' Critical Infrastructure Cyber Community (C^3) Voluntary Program launched the same day.
- May 14, 2014: Agencies responsible for regulating security of critical infrastructure must propose "prioritized, risk-based, efficient, and coordinated actions . . . to mitigate cyber risk" if they have previously determined that current regulatory requirements are insufficient. § 10(b)

VENABLE LLP

Cybersecurity Framework

Basics of the Cybersecurity Framework

- Leverages existing cybersecurity best practices (ISO 27001/2, SP800-53, COBIT, ISA 99, etc.).
- Controls divided into five "core functions":
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover
- Each function has categories, sub-categories, and informative references.
- Tiers represent how organizations view and respond to risk; profiles facilitate customization and improvement.

VENABLE LLP

Cybersecurity Framework

Notable Changes from Preliminary Version

- Removal of separate privacy appendix; integration of methodology into the body of the Framework.
- Increased focus on business case for cyber risk management ("bottom line," "overinvestment," "business needs," "economies of scale").
- Increased focus on flexibility.
- Tweaking of subcategories.
  - Removal of IP-specific control
  - Removal of "PII" control
  - Addition of language on network segregation

VENABLE LLP

Cybersecurity Framework
Framework Goals

- Provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach to managing cybersecurity risk.
- Provide a common language and mechanism for risk assessment and risk management.
- Ensure senior executive-level engagement in the cybersecurity risk management process.
  - Communicating mission priorities, available resources, and overall risk tolerance
  - Incorporating cybersecurity risk assessment into overall enterprise risk management

VENABLE LLP

Cybersecurity Framework
Incentives

- For now, technical assistance via C^3.
- Federal financial incentives not close to fruition in near term.
  - DHS/White House have stated that safety is its own incentive
  - Expectation is that market-based "incentives" will develop organically (better access to insurance, trustmark-like certifications, etc.)
- Legislation needed to expand availability.

VENABLE LLP

Cybersecurity Framework
Impact on Business

- Implementation of Framework is left to entity's discretion, but some expectations are made explicit:
  - "[O]rganizations responsible for Critical Infrastructure need to have a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk."
  - In performing a self-assessment, an "organization may determine that it has opportunities to (or needs to) improve."
- Security concerns must be managed in a manner commensurate with risk.

VENABLE LLP

Cybersecurity Framework
Liability

- Some have identified potential for emerging tort liability for commercially unreasonable cybersecurity practices.
- The CF may define the cybersecurity standard of care.
- Critical Infrastructure may be held to more stringent standard due to higher expected impact of attacks.
- Corporate boards may be subject to shareholder suits following breaches/attacks if share price is affected.

VENABLE LLP

Cybersecurity Framework
Other Concerns

- Will there be certification/audit requirements to qualify for incentives?
- How will insurers make use of the Framework? An upcoming *Request for Information* will help answer this.
- Will agencies base new regulations on the Framework per section 10 of the EO?
- Availability of quality incentives, especially liability limitation.

VENABLE LLP

Practical Implications
Industry Practices and Response

- Long-standing industry best practices
- Industry reactions to recent changes in Cybersecurity Framework and other regulations
- Common pitfalls
- Opportunities for maximizing shareholder value

VENABLE LLP

How to Thrive in Cyber

10 Key Considerations

1. **Be Prepared:** Prepare and update your cyber incident response plan; have it vetted by technical and legal experts.
2. **Be Integrated:** Share cybersecurity responsibility among chief information, security, and legal executives.
3. **Be Both Secure *and* Compliant:** Consult technical *and* legal experts to address cyber risk *and* compliance issues.
4. **Be Methodical:** Demonstrate that you can translate your cybersecurity methodology to the Cybersecurity Framework.
5. **Be Audit-proof:** Perform internal audits often; your cybersecurity practices will be audited.

VENABLE LLP

How to Thrive In Cyber

10 Key Considerations

6. **Be Proactive:** Consult other regulated industry participants to assess best practices (*e.g.*, financial services, healthcare).
7. **Be Sure to Insure:** Understand whether and to what extent you should have cybersecurity insurance.
8. **Be Hygienic:** Incorporate basic, daily cybersecurity hygiene throughout your organization; get help to develop procedures.
9. **Be Diligent:** Have counsel review your customers' cybersecurity requirements; use Q&As for clarification.
10. **Be Open:** Share information about risks or cyber incidents; consult with technical and legal experts to mitigate risk.

VENABLE LLP

Contact Information

Your Venable Team

J. Scott Hommer, III
jshommer@Venable.com
t 703.760.1658
f 703.821.8949

Jamie Barnett, Rear Admiral (Ret.)
jbarnett@Venable.com
t 202.344.4695
f 202.344.8300

Keir X. Bancroft
kxbancroft@Venable.com
t 202.344.4826
f 202.344.8300

Jason R. Wool
jrwool@Venable.com
t 202.344.4511
f 202.344.8300

www.Venable.com

Additional Information

VENABLE LLP

government contracts update

January 2014

Please contact the authors below if you have questions regarding this alert.

Authors:

Rebecca E. Pearson
repearson@Venable.com
202.344.8183

Keir X. Bancroft
kxbancroft@Venable.com
202.344.4826

Anna E. Pulliam
aepulliam@Venable.com
703.905.1457

Time to Comply: New DoD Rules Governing Supply Chain Risk Information and Unclassified Controlled Technical Information

Government contractors should be aware of recent Department of Defense (DoD) rules governing Information Relating to Supply Chain Risk, 78 Fed. Register 69,268 (Nov. 18, 2013) and Unclassified Controlled Technical Information, 78 Fed. Register 69,273 (Nov. 18, 2013). The two key implications of the rules for Government Contractors are:

- Contractors may be removed from information technology procurements supporting national security systems for failure to satisfy standards related to supply chain risk, and in some cases they will be unable to protest their removal; and
- Contractors must safeguard unclassified controlled technical information (UCTI) and take quick action to report and investigate "cyber incidents" having an actual or potential adverse effect on UCTI.

Though contractors **have until January 17, 2014 to comment** on the interim rule on safeguarding UCTI, the rules are presently in effect and apply to procurements of both commercial and noncommercial items. This update gives a summary of the rules and their implications for government contractors.

Supply Chain Risk Information Requirements

Section 806 implementation

The DoD's interim rule, "Requirements for Information Relating to Supply Chain Risk," implements Section 806 of the National Defense Authorization Act (NDAA) for Fiscal Year 2011 authorizing DoD officials to restrict certain sources of supply from information technology procurements supporting national security systems if they pose supply chain risk. Section 806 defines supply chain risk as a risk that:

> *"An adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a national security system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system*."

Authority to exclude sources of supply

Under a DoD pilot program authorized by Section 806, the Secretaries of Defense, the Army, the Navy, the Air Force, or a limited number of designees may mitigate supply chain risk by:

- Excluding sources of supply from covered procurements if they fail to meet qualification standards established in accordance with 10 U.S.C. § 2319;
- Excluding any source of supply that fails to achieve an acceptable rating with regard to an evaluation factor providing for the consideration of supply chain risk in the evaluation of proposals; and
- Withholding consent for a contractor to subcontract with a particular source or supply, or direct a contractor for a covered system to exclude a particular source from consideration for a subcontract under the contract.

In determining whether to take these actions, the authorized officials may consider public and non-public information, including all-source intelligence, relating to an offeror and its supply chain.

Information withholding authorized

The interim rule lacks clarity as to what "qualification standards" or "evaluation factor" sources of supply must satisfy to comply with the rule. Contractors may want to consult FAR 9.2, Qualifications Requirements, for details on how agencies currently implement qualifications requirements under Section 2319. However, authorized officials may limit disclosure of information relating to the basis for excluding certain sources of supply from procurements under the interim rule. In such cases, these actions are not subject to review before the Government Accountability Office or any federal court. These officials are also required to communicate with other federal agencies about other procurements that may be subject to the same supply chain risk.

Applicable to IT procurements supporting national security systems

Though the rule will be applied to a specific subset of national security systems, all DoD components are required to incorporate DFARS Clause 252.239-7017, Notice of Supply Chain Risk, *in all solicitations involving the development or delivery of any information technology* – whether acquired as a service or as a supply – including commercial item procurements, falling both above and below the simplified acquisition threshold. The national security systems under the interim rule:

- Support intelligence activities; cryptologic activities related to national security; the command and control of military forces; and equipment integral to weapon or weapons systems;
- Are critical to direct fulfillment of military or intelligence missions (but do not include systems used for routine administrative and business applications);
- Are protected as classified by Executive Order or an Act of Congress in the interest of national defense or foreign policy.

Tips for contractors

Contractors providing information technology supplies or services should consider the following:

- Contractors are required under the interim rule to "maintain controls in the provision of supplies and services to the Government to minimize supply chain risk."
- Agencies may consider all sources of information in determining supply chain risk; contractors should therefore perform diligence to ascertain if they might trigger a supply chain risk.
- Contractors should perform due diligence on supply chain subcontractors, which may be individually excluded from national security system information technology procurements.

Consider submitting written comments on the rule, which are due by January 17, 2014.

Safeguarding Unclassified Controlled Technical Information

Contractors must also comply with the DoD's final rule requiring the safeguarding of unclassified controlled technical information that is either resident on or transiting through contractors' unclassified information systems. DoD defines UCTI as technical data or computer software with military or space application that the Department has marked as controlled in accordance with DoD Instruction 5230.24, which covers Distribution Statements on Technical Documents.

Required preventative security measures

Under the rule, a contractor must enact safeguards to provide "adequate security" to its project, enterprise, or company-wide unclassified information technology systems to prevent compromise of UCTI. The DoD adopts information security controls prescribed by the National Institutes of Standards and Technology (NIST) as a baseline for ensuring adequate security. Under the rule, a contractor can choose from among the following options:

- Implement specific security controls and methodologies set forth in NIST Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations;
- Convince the DoD that some or all of the specified SP 800-53 security controls are inapplicable; or
- Demonstrate that the contractor has applied alternative and equivalent security measures.

To ensure adequate security, DoD requires that contractors use "protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information." To that end, if a contractor determines additional security measures beyond the SP 800-53 or equivalent controls are necessary, they must be applied.

Cyber incident reporting requirements

The rule requires contractors to report any "cyber incident" that results in an *actual or potentially adverse effect* on an information system or the information residing on it. A cyber incident includes any exfiltration (including the unauthorized release or copying of data), manipulation, other loss or compromise of UCTI on a contractor or its subcontractor's systems. Contractors must also report any unauthorized access to systems on which UCTI resides.

- Within 72 hours of a cyber incident, a contractor must report to DoD a number of details, which include:
- The type of compromise (for example, unauthorized access or inadvertent release);
- Contracts and DoD programs affected;
- Identification of the technical information compromised;
- The name and CAGE code of the subcontractor if this was an incident on a subcontractor network;
- Date and location of the incident; and
- Any additional pertinent information.

It is important to note that the rule mandates reporting regardless of whether a cyber incident has an actual or a possible adverse effect on UCTI. This language indicates contractors will have to submit reports to DoD within the 72 hour window even if they have not been able to confirm whether there was an actual exfiltration or compromise of UCTI.

Damage assessment support

After reporting a cyber incident, the contractor must also support the DoD's damage assessment by identifying the specific computers, information systems, and UCTI compromised. For at least 90 days from the date of the cyber incident, the contractor must preserve and protect images of known affected information systems and all relevant monitoring or packet capture data so the DoD may use it if it elects to conduct a damage assessment.

Subcontractors and outsourced IT infrastructure

The rule applies equally to subcontractors; DoD mandates the substance of the UCTI safeguarding requirements be flowed down to subcontracts, even those involving commercial items. In fact, the DoD clarified when promulgating the final rule that IT infrastructure services such as Internet Service Providers (ISPs) and cloud service providers will count as subcontractors for purposes of compliance with the rule. 78 Fed. Register 69,274.

Assessing compliance; no safe harbor provisions

The rule states that the contracting officer, after consulting with a "security manager" of a requiring activity will assess a contractor's compliance with the rule in the event of a cyber incident. The rule clarifies that though the report of a cyber incident is not enough in itself to constitute evidence that the contractor failed to provide adequate information safeguards for UCTI, or otherwise failed to comply with the rule, it will be considered as part of the contracting officer's overall assessment of the contractor's compliance with safeguarding requirements. DoD also states in the discussion and analysis of the rule that audits or reviews of contract compliance will be conducted at the discretion of the contracting officer in accordance with the terms of the contract. 78 Fed. Register 69,274. The DoD also clarifies that it does not intend the reporting obligation to constitute a safe harbor statement. *Id*. at 69,278.

Defining UCTI and prescribing marking requirements

The DoD re-scoped its rule by focusing on controlled *technical* information. Earlier proposed rules were applicable to the more general category of controlled unclassified information (CUI), but DoD focused on controlled technical information, which it "determined to be of utmost importance and which DoD has existing authority to protect." 78 Fed. Register at 69,274. DoD defines "controlled technical information" as:

> *"Technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, or dissemination."*

DoD elaborates in its rule that controlled technical information is marked in accordance with distribution statements B through F under DoD Instruction 5230.24, Distribution Statements on Technical Documents, and expressly excludes from its definition information that is *lawfully publicly available without restrictions*. The rule also further defines the term "technical information" as technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data – Non Commercial Items, and clarifies those definitions apply regardless of whether or not the clause is incorporated in the solicitation or contract. Some examples of technical information include:

- research and engineering data
- engineering drawings and associated lists
- specifications
- standards
- catalog-item identifications
- data sets
- studies
- analyses

- process sheets
- manuals
- technical reports and orders
- computer software executable code
- source code

Applicable to all solicitations and contracts

The requirement at DFARS 204.7303 specifies that the new clause at 252.204-7012, Safeguarding of Unclassified Controlled Technical Information, must be used in all solicitations and contracts, including contracts for commercial items. Thus, contractors should be mindful that any new DoD procurements will include this requirement.

Tips for contractors

Any contractors hosting UCTI on their servers, or that may have UCTI transiting through their servers, or have subcontractors or IT infrastructure providers doing the same, should consider the following:

- The rule applies to information systems at the project, enterprise, or business level. Contractors must accurately assess the scope of systems with which UCTI will have any contact; that will help clarify the information systems against which this rule applies. The scope of information systems in question will likely contribute to the allowability of compliance costs. The DoD stated in its discussion and analysis of the rule that "this contract requirement will be spread across and benefitting multiple contracts" and as a result "costs associated with implementation will be allowable and chargeable to indirect costs pools." 78 Fed. Register at 69,275. That being the case, contractors should consider the cost of project-scoped information systems, as the DoD stated that it "does not intend to directly pay for the operating costs associated with the rule."
- The rule applies to subcontractors and third-party IT infrastructure providers; contractors should be sure their subcontracts and service agreements reflect all of the DoD's UCTI requirements.
- The rule requires reporting cyber incidents that have actual or potential adverse effects on UCTI; contractors must be prepared to notify their clients within 72 hours of a cyber incident, even if they have not confirmed there were actual adverse effects on UCTI.
- The rule requires contractors to provide a significant amount of assistance to DoD in identifying and assessing the effects of a cyber incident; contractors should be sure they have the resources available to satisfy these requirements in the months following a cyber incident.

If there is any doubt, contractors should seek confirmation with a contracting officer as to whether a certain type of information falls within the category of UCTI. A contracting officer, with the assistance of only a "security manager" whose responsibilities and authority are not clarified under the rule, has a great deal of discretion in determining if a contractor complied with the requirements under this rule. Thus, contractors should be proactive with their contracting officer to determine the boundaries of compliance.

For assistance in determining how these regulations might impact your business, please contact **Becky Pearson** at repearson@Venable.com, **Keir Bancroft** at kxbancroft@Venable.com, **Anna Pulliam** at aepulliam@Venable.com, or any of the other attorneys in Venable's **Government Contracts Practice Group**.

FEDERAL REGISTER

Vol. 78 Monday,
No. 222 November 18, 2013

Part III

Department of Defense

Defense Acquisition Regulations System

48 CFR Parts 204, 208, 212 et al.
Defense Federal Acquisition Regulation Supplement; Interim Rule and Final Rules

DEPARTMENT OF DEFENSE

Defense Acquisition Regulations System

48 CFR Parts 208, 212, 215, 233, 239, 244, and 252

RIN 0750–AH96

Defense Federal Acquisition Regulation Supplement: Requirements Relating to Supply Chain Risk (DFARS Case 2012–D050)

AGENCY: Defense Acquisition Regulations System, Department of Defense (DoD).

ACTION: Interim rule.

SUMMARY: DoD is issuing an interim rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to implement a section of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2011, as amended by the NDAA for FY 2013. This interim rule allows DoD to consider the impact of supply chain risk in specified types of procurements related to national security systems.

DATES: *Effective* November 18, 2013.

Comment date: Comments on the interim rule should be submitted in writing to the address shown below on or before January 17, 2014, to be considered in the formation of a final rule.

ADDRESSES: Submit comments identified by DFARS Case 2012–D050, using any of the following methods:

- *Regulations.gov: http://www.regulations.gov.* Submit comments via the Federal eRulemaking portal by entering ''DFARS Case 2012–D050'' under the heading ''Enter keyword or ID'' and selecting ''Search.'' Select the link ''Submit a Comment'' that corresponds with ''DFARS Case 2012–D050.'' Follow the instructions provided at the ''Submit a Comment'' screen. Please include your name, company name (if any), and ''DFARS Case 2012–D050'' on your attached document.
- *Email:* dfars@osd.mil. Include DFARS Case 2012–D050 in the subject line of the message.
- *Fax:* 571–372–6094.
- *Mail:* Defense Acquisition Regulations System, Attn: Dustin Pitsch, OUSD(AT&L)DPAP/DARS, Room 3B855, 3060 Defense Pentagon, Washington, DC 20301–3060.

Comments received generally will be posted without change to *http://www.regulations.gov,* including any personal information provided. To confirm receipt of your comment(s), please check *www.regulations.gov,* approximately two to three days after submission to verify posting (except allow 30 days for posting of comments submitted by mail).

FOR FURTHER INFORMATION CONTACT: Dustin Pitsch, Defense Acquisition Regulations System, OUSD(AT&L)DPAP/DARS, Room 3B855, 3060 Defense Pentagon, Washington, DC 20301–3060, telephone 571–372–6090.

SUPPLEMENTARY INFORMATION:

I. Background

This interim rule amends the DFARS to implement section 806 of the National Defense Authorization Act for Fiscal Year 2011 (Pub. L. 111–383), entitled ''Requirements for Information Relating to Supply Chain Risk,'' as amended by section 806 of the NDAA for FY 2013 (Pub. L. 112–239), and allows DoD to consider the impact of supply chain risk in specified types of procurements related to national security systems. Section 806 defines supply chain risk as ''the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.''

II. Discussion and Analysis

This DFARS change is necessary to implement the authorities provided to DoD by section 806, enabling DoD to establish a pilot program to mitigate supply chain risk, which is set to expire on September 30, 2018. These authorities are in addition to other available mitigations, which may not be adequate to protect against the malicious actions referred to in the definition of supply chain risk.

Section 806 actions are permitted in procurements related to National Security Systems (NSS) (see 44 U.S.C. 3542(b)) that include a requirement relating to supply chain risk. This rule implements section 806's three supply-chain risk-management approaches as follows:

(1) The exclusion of a source that fails to meet qualification standards established in accordance with the requirements of 10 U.S.C. 2319, for the purpose of reducing supply chain risk in the acquisition of covered systems.

(2) The exclusion of a source that fails to achieve an acceptable rating with regard to an evaluation factor providing for the consideration of supply chain risk in the evaluation of proposals for the award of a contract or the issuance of a task or delivery order.

(3) The decision to withhold consent for a contractor to subcontract with a particular source or to direct a contractor for a covered system to exclude a particular source from consideration for a subcontract under the contract.

The rule establishes a new provision and clause (see DFARS 239.7306) for inclusion in all solicitations and contracts, including contracts for commercial items or commercial off-the-shelf items involving the development or delivery of any information technology, whether acquired as a service or as a supply, because portions of these contracts may be used to support or link with one or more NSS. Another reason for including the provision and clause in all DoD solicitations and contracts for information technology is to manage the operational security risks of including the provision and clause only in procurements for very sensitive DoD procurements, thereby identifying those very procurements as a target for the risk section 806 aims to deter.

However, several limiting provisions exist before the Government can exercise its authorities under section 806. First, use of section 806 authorities is limited to the procurement of NSS or of covered items of supply used within NSS. Section 806 defines a ''covered item of supply'' as ''an item of information technology . . . that is purchased for inclusion in (an NSS), and the loss of integrity of which could result in a supply chain risk'' to the entire system. Therefore, though the clause will be inserted in all information-technology contracts, these authorities will not be able to be utilized for all information and communication technology in all systems, but rather only in those meeting the criteria stated above.

Second, the decision to exclude a source under section 806 can only be made by the ''head of a covered agency,'' limited by definition to the Secretary of Defense and the Secretaries of the military departments with delegation limited to officials at or above the level of the service acquisition executive for the agency.

Third, the head of a covered agency seeking to exercise the authority of section 806 must obtain a joint recommendation from the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) and the Chief Information Officer of the Department of Defense (DoD CIO), based on a risk assessment from the Under Secretary of Defense for Intelligence

(USD(I)) that there is significant supply chain risk to a particular NSS.

Fourth, the head of a covered agency, with the concurrence of the USD(AT&L), must make a written determination that the use of section 806 authority is ''necessary to protect national security by reducing supply chain risk'' and that ''less intrusive measures are not reasonably available to reduce such supply chain risk.''

Fifth, notice of each determination to exercise section 806 authorities must be provided in advance to the appropriate congressional committees.

Finally, section 806 expires on September 30, 2018 (see section 806 of FY 2013 NDAA, Public Law 112–239).

Section 806 also provides that the head of a covered agency may ''limit, notwithstanding any other provision of law, in whole or in part, the disclosure of information relating to the basis for carrying out a covered procurement action'' if the head of a covered agency, with the concurrence of the USD (AT&L), determines in writing that ''the risk to national security due to disclosure of such information outweighs the risk due to not disclosing such information.''

If the Government exercises the authority provided to limit disclosure of information, no action undertaken by the Government under such authority shall be subject to review in a bid protest before the Government Accountability Office or in any Federal court.

III. Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This is a significant regulatory action and, therefore, was subject to review under section 6(b) of E.O. 12866, Regulatory Planning and Review, dated September 30, 1993. This rule is not a major rule under 5 U.S.C. 804.

IV. Regulatory Flexibility Act

DoD does not expect this interim rule to have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601, et seq., because companies have an existing interest in having a supply chain that it can rely on to provide it with material and supplies that allow the contractor to ultimately supply its customers with products that are safe and that do not impose threats or risks to government information systems.

However, an Initial Regulatory Flexibility Analysis (IRFA) has been prepared because there is a growing interest by both the Government and industry in establishing cost efficient ways to protect the supply chain related to information technology purchases. Congress has recognized a growing concern for risks to the supply chain for technology contracts supporting the Department of Defense (DoD). Congress has defined supply chain risk as ''the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.'' (See section 806(e)(4) of Pub. L. 111–383.)

The objective of this rule is to protect DoD against risks arising out of the supply chain.

The legal basis for this rule is section 806 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2011 (Pub. L. 111–383), as amended by section 806 of the NDAA for FY 2013 (Pub. L. 112–239). Additionally, the Department of Defense Instruction (DoDI) 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), recognizes the need to improve supply chain risk management (SCRM). In doing so, the DoDI requires, among other things, implementation of section 806 in the DFARS and in appropriate solicitation and contract language.

This rule applies to contractors involved in the development or delivery of any information technology, whether acquired by DoD as a service or as a supply. This includes commercial purchases as well as purchases of commercial off-the-shelf (COTS) services or supplies.

This rule does not require any specific reporting, recordkeeping or compliance requirements. It does, however, recognize the need for information technology contractors to implement appropriate safeguards and countermeasures to minimize supply chain risk. This rule, by itself, does not require contractors to deploy additional supply chain risk protections, but leaves it up to the individual contractors to take the steps they think are necessary to maintain existing or otherwise required safeguards and countermeasures as necessary for their own particular industrial methods to protect their supply chain.

The rule does not duplicate, overlap, or conflict with any other Federal rules.

Consistent with the stated objectives of section 806 and the DoDI, no viable alternatives exist.

Possible alternatives considered included having all contractors report, on all contracts, the nature of the supply chain risk mitigation efforts they have applied to their manufacturing processes. This would be unduly burdensome for both contractors and the Government.

Another alternative is not to have section 806 clauses apply to commercial and COTS items or purchases below the simplified acquisition threshold. However, the requirements of section 806 should apply to contracts and subcontracts at or below the simplified acquisition threshold because the malicious introduction of unwanted functions may occur at any dollar threshold. Therefore, it would not be in the best interest of the Federal Government to exempt contracts and subcontracts at or below the simplified acquisition threshold from this requirement.

In a like manner, the requirements of section 806 should apply to the procurement of commercial items (including COTS items) because the intent of the statute is to protect the supply chain which in turn protects all NSS. Commercial and COTS information technology supplies and services often become part of NSSs. Protection of the NSSs using the authority of section 806 requires application in all information technology supply and services contacts. Therefore, exempting commercial (including COTS) items from application of the statute would negate the intended effect of the statute.

DoD invites comments from small business concerns and other interested parties on the expected impact of this rule on small entities.

DoD will also consider comments from small entities concerning the existing regulations in subparts affected by this rule in accordance with 5 U.S.C. 610. Interested parties must submit such comments separately and should cite 5 U.S.C. 610 (DFARS Case 2012–D050) in correspondence.

V. Paperwork Reduction Act

The rule does not contain any information collection requirements that require the approval of the Office of Management and Budget under the

Paperwork Reduction Act (44 U.S.C. chapter 35.

VI. Determination To Issue an Interim Rule

A determination has been made under the authority of the Secretary of Defense that urgent and compelling reasons exist to promulgate this interim rule without prior opportunity for public comment. This action is necessary because of the urgent need to protect the National Security Systems (NSS) and the integrity of the supply chain to NSS. It is necessary to reduce supply chain risk in the acquisition of sensitive information technology systems that are used for intelligence or cryptologic activities; used for command and control of military forces; or from an integral part of a weapon system by avoiding sabotage, maliciously introducing unwanted functions, or other subversion of the design, integrity, manufacturing, production, installation, operation or maintenance of systems. Such acquisition decisions are made daily and, like other cybersecurity measures, the costs to mitigate supply chain risk after a system is already in operation can be very high. In addition, as this is a pilot authority set to expire on September 30, 2018, and the Congress has requested a report on the effectiveness of the authority not later than January 1, 2017, therefore DoD must make this tool available immediately to begin the pilot program and gather feedback for the report to Congress.

The globalization of information technology has increased the vulnerability of DoD to attacks on its systems and networks. Failure to implement this rule may cause harm to the Government and to individuals relying on the integrity of NSS, for example, the risk of allowing the malicious insertion of software code or an unwanted function designed to degrade DOD's sensitive systems. DoD has proceeded cautiously to ensure that this rule very closely mirrors the authorities provided in the statute and has little leeway to vary from those terms. However, pursuant to 41 U.S.C. 1707 and FAR 1.501–3(b), DoD will consider public comments received in response to this interim rule in the formation of the final rule.

List of Subjects in 48 CFR Parts 208, 212, 215, 233, 239, 244, and 252

Government procurement.

Manuel Quinones,

Editor, Defense Acquisition Regulations System.

Therefore, 48 CFR parts 208, 212, 215, 233, 239, 244, and 252 are amended as follows:

■ 1. The authority citation for 48 CFR parts 208, 212, 215, 233, 239, 244, and 252 continues to read as follows:

Authority: 41 U.S.C. 1303 and 48 CFR Chapter 1.

PART 208—REQUIRED SOURCES OF SUPPLIES AND SERVICES

■ 2. Add section 208.405 to read as follows:

208.405 Ordering procedures for Federal Supply Schedules.

In all orders and blanket purchase agreements involving the development or delivery of any information technology, whether acquired as a service or as a supply, consider the need for an evaluation factor regarding supply chain risk (see subpart 239.73).

■ 3. Amend section 208.7402 by—

■ a. Designating the text as paragraph (1); and

■ b. Adding new paragraph (2) to read as follows:

208.7402 General.

(1) * * *

(2) In all orders and blanket purchase agreements involving the development or delivery of any information technology, whether acquired as a service or as a supply, consider the need for an evaluation factor regarding supply chain risk (see subpart 239.73).

PART 212—ACQUISITION OF COMMERCIAL ITEMS

■ 4. Amend section 212.301 by—

■ a. Revising paragraph (f)(xiv);

■ b. Redesignating—

■ i. Paragraphs (f)(liii) through (lxv) as (lvi) through (lxvii); and

■ ii. Paragraphs (f)(xv) through (lii) as (f)(xvi) through (liii).

■ c. Adding new paragraphs (f)(xv), (liv), and (lv).

Revision and additions to read as follows:

212.301 Solicitation provisions and contract clauses for the acquisition of commercial items.

(f) * * *

(xiv) Use the provision 252.215–7008, Only One Offer, as prescribed at 215.408(4);

(xv) Use the clause at 252.219–7003, Small Business Subcontracting Plan (DoD Contracts), as prescribed in 219.708(b)(1)(A)(*1*), to comply with 15 U.S.C. 637. Use the clause with its Alternate I when prescribed in 219.708(b)(1)(A)(*2*).

* * * * *

(liv) Use the provision at 252.239–7017, Notice of Supply Chain Risk, as prescribed in 239.7306(a), to comply with section 806 of Public Law 111–383, in all solicitations for contracts involving the development or delivery of any information technology, whether acquired as a service or as a supply.

(lv) Use the clause at 252.239–7018, Supply Chain Risk, as prescribed in 239.7306(b), to comply with section 806 of Public Law 111–383, in all solicitations and contracts involving the development or delivery of any information technology, whether acquired as a service or as a supply.

* * * * *

PART 215—CONTRACTING BY NEGOTIATION

■ 5. Amend section 215.304 by adding new paragraph (c)(v) to read as follows:

215.304 Evaluation factors and significant subfactors.

(c) * * *

(v) In all solicitations and contracts involving the development or delivery of any information technology, whether acquired as a service or as a supply, consider the need for an evaluation factor regarding supply chain risk (see subpart 239.73).

■ 6. Add new subpart 215.5 to read as follows:

Subpart 215.5—Preaward, Award, and Postaward Notifications, Protests, and Mistakes

Sec.

215.503 Notifications to unsuccessful offerors.

215.506 Postaward debriefing of offerors.

Subpart 215.5—Preaward, Award, and Postaward Notifications, Protests, and Mistakes

215.503 Notifications to unsuccessful offerors.

If the Government exercises the authority provided in 239.7305(d), the notifications to unsuccessful offerors, either preaward or postaward, shall not reveal any information that is determined to be withheld from disclosure in accordance with section 806 of the National Defense Authorization Act for Fiscal Year 2011, as amended by section 806 of the

National Defense Authorization Act for Fiscal Year 2013 (see subpart 239.73).

215.506 Postaward debriefing of offerors.

(e) If the Government exercises the authority provided in 239.7305(d), the debriefing shall not reveal any information that is determined to be withheld from disclosure in accordance with section 806 of the National Defense Authorization Act for Fiscal Year 2011, as amended by section 806 of the National Defense Authorization Act for Fiscal Year 2013 (see subpart 239.73).

PART 233—PROTESTS, DISPUTES, AND APPEALS

■ 7. Add new section 233.102 to read as follows:

233.102 General.

If the Government exercises the authority provided in 239.7305(d) to limit disclosure of information, no action undertaken by the Government under such authority shall be subject to review in a bid protest before the Government Accountability Office or in any Federal court (see subpart 239.73).

PART 239—ACQUISITION OF INFORMATION TECHNOLOGY

■ 8. Add new subpart 239.73 to read as follows:

Subpart 239.73—Requirements for Information Relating to Supply Chain Risk

Sec.

Subpart 239.73—Requirements for Information Relating to Supply Chain Risk

239.7300 Scope of subpart.

(a) This subpart implements section 806 of the National Defense Authorization Act for Fiscal Year 2011 (Pub. L. 111–383) and elements of DoD Instruction 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), at (*http://www.dtic.mil/whs/directives/corres/pdf/520044p.pdf*).

(b) The authority provided in this subpart expires on September 30, 2018 (see section 806(a) of Pub. L. 112–239).

239.7301 Applicability.

Notwithstanding FAR 39.001, this subpart shall be applied to acquisition of information technology for national security systems, as that term is defined at 44 U.S.C. 3542(b), for procurements involving—

(a) A source selection for a covered system or a covered item involving either a performance specification (see 10 U.S.C. 2305(a)(1)(C)(ii)), or an evaluation factor (see 10 U.S.C. 2305(a)(2)(A)), relating to supply chain risk;

(b) The consideration of proposals for and issuance of a task or delivery order for a covered system or a covered item where the task or delivery order contract concerned includes a requirement relating to supply chain risk (see 10 U.S.C. 2304c(d)(3) and FAR 16.505(b)(1)(iv)(D)); or

(c) Any contract action involving a contract for a covered system or a covered item where such contract includes a requirement relating to supply chain risk.

239.7302 Definitions.

As used in this subpart—

Covered item means an item of information technology that is purchased for inclusion in a covered system, and the loss of integrity of which could result in a supply chain risk for a covered system (see section 806(e)(6) of Pub. L. 111–383).

Covered system means a national security system, as that term is defined at 44 U.S.C. 3542(b) (see section 806(e)(5) of Pub. L. 111–38). It is any information system, including any telecommunications system, used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

(1) The function, operation, or use of which—

(i) Involves intelligence activities;

(ii) Involves cryptologic activities related to national security;

(iii) Involves command and control of military forces;

(iv) Involves equipment that is an integral part of a weapon or weapons system; or

(v) Is critical to the direct fulfillment of military or intelligence missions but this does not include a system that is to be used for routine administrative and business applications, including payroll, finance, logistics, and personnel management applications; or

(2) Is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Information technology, in lieu of the definition at FAR 2.1, and *supply chain risk,* are defined in the clause at 252.239–7018, Supply Chain Risk.

239.7303 Authorized individuals.

(a) Subject to 239.7304, the following individuals are authorized to take the actions authorized by 239.7305:

(1) The Secretary of Defense.

(2) The Secretary of the Army.

(3) The Secretary of the Navy.

(4) The Secretary of the Air Force.

(b) The individuals authorized at paragraph (a) may not delegate the authority to take the actions at 239.7305 or the responsibility for making the determination required by 239.7304 to an official below the level of—

(1) For the Department of Defense, the Under Secretary of Defense for Acquisition, Technology, and Logistics; and,

(2) For the military departments, the senior acquisition executive for the department concerned.

239.7304 Determination and notification.

The individuals authorized in 239.7303 may exercise the authority provided in 239.7305 only after—

(a) Obtaining a joint recommendation by the Under Secretary of Defense for Acquisition, Technology, and Logistics and the Chief Information Officer of the Department of Defense, on the basis of a risk assessment by the Under Secretary of Defense for Intelligence, that there is a significant supply chain risk to a covered system;

(b) Making a determination in writing, in unclassified or classified form, with the concurrence of the Under Secretary of Defense for Acquisition, Technology, and Logistics, that—

(1) Use of the authority in 239.7305(a)(b) or (c) is necessary to protect national security by reducing supply chain risk;

(2) Less intrusive measures are not reasonably available to reduce such supply chain risk; and

(3) In a case where the individual authorized in 239.7303 plans to limit disclosure of information under 239.7305(d), the risk to national security due to the disclosure of such information outweighs the risk due to not disclosing such information; and

(c)(1) Providing a classified or unclassified notice of the determination made under paragraph (b) of this section—

(i) In the case of a covered system included in the National Intelligence Program or the Military Intelligence Program, to the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the congressional defense committees; and

(ii) In the case of a covered system not otherwise included in paragraph (a) of this section, to the congressional defense committees; and

(2) The notice shall include—

(i) The following information (see 10 U.S.C. 2304(f)(3)):

(A) A description of the agency's needs.

(B) An identification of the statutory exception from the requirement to use competitive procedures and a demonstration, based on the proposed contractor's qualifications or the nature of the procurement, of the reasons for using that exception.

(C) A determination that the anticipated cost will be fair and reasonable.

(D) A description of the market survey conducted or a statement of the reasons a market survey was not conducted.

(E) A listing of the sources, if any, that expressed in writing an interest in the procurement.

(F) A statement of the actions, if any, the agency may take to remove or overcome any barrier to competition before a subsequent procurement for such needs;

(ii) The joint recommendation by the Under Secretary of Defense for Acquisition, Technology, and Logistics and the Chief Information Officer of the Department of Defense as specified in paragraph (a);

(iii) A summary of the risk assessment by the Under Secretary of Defense for Intelligence that serves as the basis for the joint recommendation specified in paragraph (a); and

(iv) A summary of the basis for the determination, including a discussion of less intrusive measures that were considered and why they were not reasonably available to reduce supply chain risk.

239.7305 Exclusion and limitation on disclosure.

Subject to 239.7304, the individuals authorized in 239.7303 may, in the course of conducting a covered procurement—

(a) Exclude a source that fails to meet qualification standards established in accordance with the requirements of 10 U.S.C. 2319, for the purpose of reducing supply chain risk in the acquisition of covered systems;

(b) Exclude a source that fails to achieve an acceptable rating with regard to an evaluation factor providing for the consideration of supply chain risk in the evaluation of proposals for the award of a contract or the issuance of a task or delivery order;

(c) Withhold consent for a contractor to subcontract with a particular source or direct a contractor for a covered system to exclude a particular source from consideration for a subcontract under the contract; and

(d) Limit, notwithstanding any other provision of law, in whole or in part, the disclosure of information relating to the basis for carrying out any of the actions authorized by paragraphs (a) through (c) of this section, and if such disclosures are so limited—

(1) No action undertaken by the individual authorized under such authority shall be subject to review in a bid protest before the Government Accountability Office or in any Federal court; and

(2) The authorized individual shall—

(i) Notify appropriate parties of a covered procurement action and the basis for such action only to the extent necessary to effectuate the covered procurement action;

(ii) Notify other Department of Defense components or other Federal agencies responsible for procurements that may be subject to the same or similar supply chain risk, in a manner and to the extent consistent with the requirements of national security; and

(iii) Ensure the confidentiality of any such notifications.

239.7306 Solicitation provision and contract clause.

(a) Insert the provision at 252.239–7017, Notice of Supply Chain Risk, in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial items, that involve the development or delivery of any information technology whether acquired as a service or as a supply.

(b) Insert the clause at 252.239–7018, Supply Chain Risk, in all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items, that involve the development or delivery of any information technology whether acquired as a service or as a supply.

PART 244—SUBCONTRACTING POLICIES AND PROCEDURES

■ 9. Add new sections 244.201 and 244.201–1 to subpart 244.2 to read as follows:

244.201 Consent and advance notification requirements.

244.201–1 Consent requirements.

In all solicitations and contracts involving the development or delivery of any information technology, whether acquired as a service or as a supply, consider the need for a consent to subcontract requirement regarding supply chain risk (see subpart 239.73).

PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

■ 10. Add section 252.239–7017 to read as follows:

252.239–7017 Notice of supply chain risk.

As prescribed in 239.7306(a), use the following provision:

NOTICE OF SUPPLY CHAIN RISK (NOV 2013)

(a) *Definition. Supply chain risk,* as used in this provision, means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a national security system (as that term is defined at 44 U.S.C. 3542(b)) so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

(b) In order to manage supply chain risk, the Government may use the authorities provided by section 806 of Public Law 111–383. In exercising these authorities, the Government may consider information, public and non-public, including all-source intelligence, relating to an offeror and its supply chain.

(c) If the Government exercises the authority provided in section 806 of Pub. L. 111–383 to limit disclosure of information, no action undertaken by the Government under such authority shall be subject to review in a bid protest before the Government Accountability Office or in any Federal court.

(End of provision)

■ 11. Add section 252.239–7018 to read as follows:

252.239–7018 Supply chain risk.

As prescribed in 239.7306(b), use the following clause:

SUPPLY CHAIN RISK (NOV 2013)

(a) *Definitions.* As used in this clause—

Information technology (see 40 U.S.C 11101(6)) means, in lieu of the definition at FAR 2.1, any equipment, or interconnected system(s) or subsystem(s) of equipment, that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.

(1) For purposes of this definition, equipment is used by an agency if the equipment is used by the agency directly or is used by a contractor under a contract with the agency that requires—

(i) Its use; or

(ii) To a significant extent, its use in the performance of a service or the furnishing of a product.

(2) The term ''information technology'' includes computers, ancillary equipment

(including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

(3) The term ''information technology'' does not include any equipment acquired by a contractor incidental to a contract.

Supply chain risk means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a national security system (as that term is defined at 44 U.S.C. 3542(b)) so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

(b) The Contractor shall maintain controls in the provision of supplies and services to the Government to minimize supply chain risk.

(c) In order to manage supply chain risk, the Government may use the authorities provided by section 806 of Public Law 111–383. In exercising these authorities, the Government may consider information, public and non-public, including all-source intelligence, relating to a Contractor's supply chain.

(d) If the Government exercises the authority provided in section 806 of Public Law 111–383 to limit disclosure of information, no action undertaken by the Government under such authority shall be subject to review in a bid protest before the Government Accountability Office or in any Federal court.

(e) The Contractor shall include the substance of this clause, including this paragraph (e), in all subcontracts involving the development or delivery of any information technology, whether acquired as a service or as a supply.

(End of clause)

[FR Doc. 2013–27311 Filed 11–15–13; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Defense Acquisition Regulations System

48 CFR Parts 204, 212, and 252

RIN 0750–AG47

Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information (DFARS Case 2011–D039)

AGENCY: Defense Acquisition Regulations System, Department of Defense (DoD).

ACTION: Final rule.

SUMMARY: DoD is issuing a final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to add a new subpart and associated contract clause to address requirements for safeguarding unclassified controlled technical information.

DATES: *Effective* November 18, 2013.

FOR FURTHER INFORMATION CONTACT: Mr. Dustin Pitsch, Defense Acquisition Regulations System, OUSD(AT&L)DPAP/DARS, Room 3B855, 3060 Defense Pentagon, Washington, DC 20301–3060. Telephone 571–372–6090; facsimile 571–372–6101.

SUPPLEMENTARY INFORMATION:

I. Background

DoD published a proposed rule in the **Federal Register** at 76 FR 38089 on June 29, 2011, to implement adequate security measures to safeguard unclassified DoD information within contractor information systems from unauthorized access and disclosure, and to prescribe reporting to DoD with regard to certain cyber intrusion events that affect DoD information resident on or transiting through contractor unclassified information systems. After comments were received on the proposed rule it was decided that the scope of the rule would be modified to reduce the categories of information covered. This final rule addresses safeguarding requirements that cover only unclassified controlled technical information and reporting the compromise of unclassified controlled technical information.

Controlled technical information is technical data, computer software, and any other technical information covered by DoD Directive 5230.24, Distribution Statements on Technical Documents, at *http://www.dtic.mil/whs/directives/corres/pdf/523024p.pdf*, and DoD Directive 5230.25, Withholding of Unclassified Technical Data from Public Disclosure, at *http://www.dtic.mil/whs/directives/corres/pdf/523025p.pdf*.

Forty-nine respondents submitted public comments in response to the proposed rule.

II. Discussion and Analysis

DoD reviewed the public comments in the development of the final rule. A discussion of the comments and the changes made to the rule as a result of those comments is provided, as follows:

A. Significant Changes From the Proposed Rule

- The final rule reflects changes to subpart 204.73, in lieu of 204.74 as stated in the proposed rule, to conform to the current DFARS baseline numbering sequence. Subpart 204.73 is now titled ''Safeguarding Unclassified Controlled Technical Information''.
- New definitions are included for: ''controlled technical information'', ''cyber incident'' and ''technical information''.
- These definitions published in the proposed rule are no longer included: ''authentication,'' ''clearing information,'' ''critical program information,'' ''cyber,'' ''data,'' ''DoD information,'' ''Government information,'' ''incident,'' ''information,'' ''information system,'' ''intrusion,'' ''nonpublic information,'' ''safeguarding,'' ''threat,'' and ''voice''.
- DFARS 204.7302 is modified to account for the reduced scope to limit the application of safeguarding controls to unclassified controlled technical information, which is marked in accordance with DoD Instruction 5230.24, Distribution Statements on Technical Documents.
- The ''procedures'' section, previously at DFARS 204.7403 in the proposed rule, is no longer included.
- DFARS 204.7303, Contract Clause, prescribes only one clause, 252.204–7012, Safeguarding of Unclassified Controlled Technical Information, which is a modification of the previously proposed ''Enhanced'' safeguarding clause. The previously proposed ''Basic'' safeguarding clause is removed and the proposed controls will be implemented through FAR case 2011–020, Basic Safeguarding of Contractor Information Systems.
- A list is added specifying the 13 pieces of information required for reporting.
- The time period a contractor must retain incident information to allow for DoD to request information necessary to conduct a damage assessment or decline interest is set at 90 days in the clause at 252.204–7012(d)(4)(iii).
- Additional information regarding DoD's damage assessment activities is added at 252.204–7012(d)(5).

B. Analysis of Public Comments

1. Align With Implementation of Executive Order on Controlled Unclassified Information

Comment: Numerous respondents indicated concerns that the proposed rule for DoD unclassified information was in advance of the Governmentwide guidance that the National Archives and Records Administration is developing for controlled unclassified information (CUI). Further, they suggested that DoD delay its efforts and instead pursue alignment with the Federal CUI policy effort, in order to avoid confusion and disconnects on information categories

(including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

(3) The term ''information technology'' does not include any equipment acquired by a contractor incidental to a contract.

Supply chain risk means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a national security system (as that term is defined at 44 U.S.C. 3542(b)) so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

(b) The Contractor shall maintain controls in the provision of supplies and services to the Government to minimize supply chain risk.

(c) In order to manage supply chain risk, the Government may use the authorities provided by section 806 of Public Law 111–383. In exercising these authorities, the Government may consider information, public and non-public, including all-source intelligence, relating to a Contractor's supply chain.

(d) If the Government exercises the authority provided in section 806 of Public Law 111–383 to limit disclosure of information, no action undertaken by the Government under such authority shall be subject to review in a bid protest before the Government Accountability Office or in any Federal court.

(e) The Contractor shall include the substance of this clause, including this paragraph (e), in all subcontracts involving the development or delivery of any information technology, whether acquired as a service or as a supply.

(End of clause)

[FR Doc. 2013–27311 Filed 11–15–13; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Defense Acquisition Regulations System

48 CFR Parts 204, 212, and 252

RIN 0750–AG47

Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information (DFARS Case 2011–D039)

AGENCY: Defense Acquisition Regulations System, Department of Defense (DoD).

ACTION: Final rule.

SUMMARY: DoD is issuing a final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to add a new subpart and associated contract clause to address requirements for safeguarding unclassified controlled technical information.

DATES: *Effective* November 18, 2013.

FOR FURTHER INFORMATION CONTACT: Mr. Dustin Pitsch, Defense Acquisition Regulations System, OUSD(AT&L)DPAP/DARS, Room 3B855, 3060 Defense Pentagon, Washington, DC 20301–3060. Telephone 571–372–6090; facsimile 571–372–6101.

SUPPLEMENTARY INFORMATION:

I. Background

DoD published a proposed rule in the **Federal Register** at 76 FR 38089 on June 29, 2011, to implement adequate security measures to safeguard unclassified DoD information within contractor information systems from unauthorized access and disclosure, and to prescribe reporting to DoD with regard to certain cyber intrusion events that affect DoD information resident on or transiting through contractor unclassified information systems. After comments were received on the proposed rule it was decided that the scope of the rule would be modified to reduce the categories of information covered. This final rule addresses safeguarding requirements that cover only unclassified controlled technical information and reporting the compromise of unclassified controlled technical information.

Controlled technical information is technical data, computer software, and any other technical information covered by DoD Directive 5230.24, Distribution Statements on Technical Documents, at *http://www.dtic.mil/whs/directives/corres/pdf/523024p.pdf*, and DoD Directive 5230.25, Withholding of Unclassified Technical Data from Public Disclosure, at *http://www.dtic.mil/whs/directives/corres/pdf/523025p.pdf*.

Forty-nine respondents submitted public comments in response to the proposed rule.

II. Discussion and Analysis

DoD reviewed the public comments in the development of the final rule. A discussion of the comments and the changes made to the rule as a result of those comments is provided, as follows:

A. Significant Changes From the Proposed Rule

- The final rule reflects changes to subpart 204.73, in lieu of 204.74 as stated in the proposed rule, to conform to the current DFARS baseline numbering sequence. Subpart 204.73 is now titled ''Safeguarding Unclassified Controlled Technical Information''.
- New definitions are included for: ''controlled technical information'', ''cyber incident'' and ''technical information''.
- These definitions published in the proposed rule are no longer included: ''authentication,'' ''clearing information,'' ''critical program information,'' ''cyber,'' ''data,'' ''DoD information,'' ''Government information,'' ''incident,'' ''information,'' ''information system,'' ''intrusion,'' ''nonpublic information,'' ''safeguarding,'' ''threat,'' and ''voice''.
- DFARS 204.7302 is modified to account for the reduced scope to limit the application of safeguarding controls to unclassified controlled technical information, which is marked in accordance with DoD Instruction 5230.24, Distribution Statements on Technical Documents.
- The ''procedures'' section, previously at DFARS 204.7403 in the proposed rule, is no longer included.
- DFARS 204.7303, Contract Clause, prescribes only one clause, 252.204–7012, Safeguarding of Unclassified Controlled Technical Information, which is a modification of the previously proposed ''Enhanced'' safeguarding clause. The previously proposed ''Basic'' safeguarding clause is removed and the proposed controls will be implemented through FAR case 2011–020, Basic Safeguarding of Contractor Information Systems.
- A list is added specifying the 13 pieces of information required for reporting.
- The time period a contractor must retain incident information to allow for DoD to request information necessary to conduct a damage assessment or decline interest is set at 90 days in the clause at 252.204–7012(d)(4)(iii).
- Additional information regarding DoD's damage assessment activities is added at 252.204–7012(d)(5).

B. Analysis of Public Comments

1. Align With Implementation of Executive Order on Controlled Unclassified Information

Comment: Numerous respondents indicated concerns that the proposed rule for DoD unclassified information was in advance of the Governmentwide guidance that the National Archives and Records Administration is developing for controlled unclassified information (CUI). Further, they suggested that DoD delay its efforts and instead pursue alignment with the Federal CUI policy effort, in order to avoid confusion and disconnects on information categories

and protections, and to prevent burdensome or duplicative costs to the contractors.

Response: To date, Federal CUI policy has not yet been promulgated for Federal Government agencies and it is unknown when Federal policy will be developed for industry as it relates to CUI. This rule has been rescoped to cover safeguarding unclassified controlled technical information, which DoD has determined to be of utmost importance and which DoD has existing authority to protect.

2. Deconflict With Other Policy Memos, DoD Instructions (DoDI) or DoD Directives (DoDD)

Comment: Respondents suggested that the rule conflicts with policies including DoDI/DoDD 5230.24/5230.25, DoD 5000 series, DoD 8570.01–M, Directives (DoDD), National Industrial Security Operating Manual (NISPOM), DoD Information Assurance Certification and Accreditation Process (DIACAP), and Federal Information Security Management Act (FISMA).

Response: The DFARS rule has been adjusted to use the marking framework established by DoDI 5230.24. DoD was unable to identify any other policy conflicts with this revised rule.

Comment: Several respondents suggested that the variety of National Institute of Standards and Technology (NIST) controls from several categories leads to a wide interpretation, which will be burdensome on personnel and there were suggestions that this hurts competition as less sophisticated firms are unable to enter the market. Another respondent suggested NIST controls should not be specified, and should be selectable by the program office. A respondent suggested that a list of controls is not sufficient and context/guidance is needed.

Response: The NIST security controls identified represent the minimum acceptable level of protection, though the clause allows for flexibility. If a control is not implemented, the contractor shall submit to the contracting officer a written explanation of how either the required security control identified is not applicable, or how an alternative control or protective measure is used to achieve equivalent protection.

Comment: Several respondents variously observed that some of the DFARS requirements are more stringent than the NISPOM.

Response: This rule has requirements to protect unclassified information stored and transmitted through unclassified networks and therefore does not align with the protection requirements in the NISPOM.

3. Policy Regarding Outsourcing, Cloud Computing, Reuse, Orphaned Works Etc.

Comment: A respondent requested clarification if use of outsourced information technology (IT) infrastructure, to include use of cloud computing, constitutes a release of information to the vendor that would be covered under the restriction on releasing information outside the Contractor's organization, and, if permitted, would the outsourced vendor be required to meet the safeguarding requirements specified in the clause.

Response: An Internet Service Provider (ISP) or cloud service provider constitutes a subcontractor in this context. The contractor is responsible for ensuring that the subcontractor complies with the requirements of this rule within the scope of this rule.

Comment: A respondent suggested the proposed rule constrains reuse of DoD information between contracts, and adds unnecessary additional DoD costs.

Response: The need-to-know requirement included in the proposed rule has been removed alleviating the concern for constraints on reuse of information. This rule is deemed necessary for the protection of unclassified controlled technical information and it is understood that implementing these controls may increase costs to DoD.

4. Consequence of Noncompliance

Comment: A number of respondents commented on the lack of oversight and certification of compliance with the NIST controls in the rule.

Response: The rule does not intend to change existing penalties or remedies for noncompliance with contract requirements.

5. Government Agency Responsible for Oversight

Comment: Two respondents suggested that the rule should identify how and by which entity audits or reviews of the safeguards will be conducted.

Response: The contract administration office is responsible for ensuring that the contractor has a process in place for meeting the required safeguarding standards. Audits or reviews will be conducted at the discretion of the contracting officer in accordance with the terms of the contract.

6. Need To Clearly Categorize, Identify, and Mark

Comment: Several respondents pointed out that DoD authority to define and mark CUI/FOUO (controlled unclassified information/for official use only) is poorly explained. FOUO is used as a catchall marking in DoD and managing this as a controlled designator is not practical. DoD is responsible for specifying a process for marking basic and enhanced criteria.

Response: The final rule has been scoped to only refer to unclassified controlled technical information. Items will be marked in accordance with DoDI 5230.24.

7. Allowable Costs Under Cost Accounting Standards (CAS)

Comment: One respondent asked if the cost associated with compliance to the DFARS changes is allowable under CAS.

Response: Cost Accounting Standards address measurement, allocation and assignment of costs. FAR 31 and DFARS 231, specifically FAR 31.201–2, address the allowability of costs. There is nothing in FAR 31 or DFARS 231 that would make costs of compliance with DFARS unallowable if the costs are incurred in accordance with FAR 31.201–2. While we cannot know in advance if a company will incur costs in accordance with FAR 31.201–2, there is nothing included in the final rule that would cause or compel a company to incur costs that would be in violation of FAR 31.201–2.

Comment: Several respondents stated that DoD needs to account for/provide funding for the additional costs of implementation.

Response: Implementation of this rule may increase contractor costs that would be accounted for through the normal course of business.

8. Applicability to Commercial Items

Comment: One respondent suggested that subcontracts for commercial items should be exempt from the unclassified data restrictions added in this rule. Several respondents suggested exempting all purchases of commercially available off-the-shelf products from the data controls added by this rule.

Response: The final rule is rescoped to focus on unclassified controlled technical information. Any unclassified controlled technical information that is shared with a contractor or subcontractor must be protected in accordance with the terms of the contract.

9. Threat Sharing

Comment: A number of respondents were concerned that if the DoD did not provide threat information to companies then they would be unable to determine adequate security for the controlled information.

Response: 32 CFR part 236 provides a voluntary framework for eligible companies to exchange cyber threat information with the Government. Threat information is not needed to determine adequate security; the select NIST 800–53 controls in clause 252.204–7012, or their equivalent as suggested by the contractor, are required for adequate security. In cases where the contractor has information (either obtained from DoD or any other source) that would suggest additional security is required to adequately protect technical information, they must take action to establish that additional security.

10. Sharing of Liability Between the Contractor and DoD

Comment: A number of respondents were concerned that the contractor will assume the full cost and liability burden for costs associated with compliance with the rule.

Response: In many cases, this contract requirement will be spread across and benefiting multiple contracts—costs associated with implementation will be allowable and chargeable to indirect cost pools. The Government does not intend to directly pay for the operating costs associated with the rule.

11. Concern for Creating Two Types of Unclassified (Basic and Enhanced)

Comment: A respondent indicated that, under the proposed rule, all Government unclassified information must be compartmentalized in order to effectively enforce need-to-know discipline. In addition, however, the proposed rule recognized two classes of information, one warranting ''basic'' protection and the second requiring ''enhanced'' protection. Further, the respondent indicated that the rule not only lacks clarity regarding identification and marking of the information to be protected, but also for designating the information as basic or enhanced. Additionally, the respondents recommended that uniform protocols need to be established, so documents can be sorted electronically into the proper categories.

Response: The final rule clarifies that contractors are required to protect one category of unclassified information, which was previously specified within the enhanced safeguarding clause. A proposed rule addressing ''basic'' safeguarding was published in the **Federal Register** on Friday, August 24, 2012 (FAR 2011–020).

12. Applicability to Foreign Contractors

Comment: One respondent was concerned about the impact of the rule on foreign contractors and on international information sharing agreements.

Response: The technical information covered by the rule is already subject to dissemination controls that existing agreements would have to have accounted for. This rule does not have an impact on those information sharing agreements. In addition, the reporting associated with the rule is specifically focused on the information that was lost, not the cyber forensic aspects of an incident.

13. Applicability to Universities

Comment: NIST SP 800–53 controls are inappropriate for academic settings and burdensome.

Response: Academic institutions dealing with unclassified controlled technical information are not exempt from the controls of this rule. The protection of the information is equally necessary, regardless of whether the contractor is a university or a business concern.

14. Scope (204.7400 Redesignated 204.7300)

Comment: The respondents recommend that this rule explicitly apply to systems containing controlled information and not the general information technology environment.

Response: The rule has been revised to apply to systems that have unclassified controlled technical information resident on or transiting through them.

Comment: Several respondents made suggestions on the scope of the proposed DFARS section 204.7400 including: university fundamental research should be exempt, the rule should apply only to new contracts, the safeguards should apply to Voice over Internet Protocol (VoIP), and the protected information should be more specific and limited.

DoD will not modify the Disclosure of Information clause at DFARS 252.204–7000 in this rule. The clause at 252.204–7012 has been revised to apply to all contracts expected to be dealing with controlled technical information. Implementation of the rule does not direct modification of existing contracts. The clause does not apply to voice information, because voice information does not fall within the definition of controlled technical information.

15. Definitions (204.7401 Redesignated 204.7301)

Comment: One respondent suggested adding the definition for ''intrusion'' at DFARS 204.7401 in addition to where it already exists in the clause proposed at 252.204–70XX or adding a pointer to refer to the clause for definitions.

Response: The definition of ''intrusion'' has been deleted because the term is no longer used in the case.

16. Policy (204.7402 Redesignated 204.7302)

Comment: Two respondents stated that the phrase ''adequate security'' and ''certain cyber incidents'' are too vague and need clarification. Another respondent stated that the enhanced safeguarding requirements in the clause 252.204–70YY are too stringent for unclassified information and compliance would be a substantial burden.

Response: The term ''adequate security'' is modified from the proposed rule to provide clarity. The final rule lays out the policy and definitions for the terms ''adequate security'' and ''cyber incident''. The criteria for reporting a cyber incident is established within the clause at 252.204–7012. DoD has determined that unclassified controlled technical information is vital to national security and must be protected.

17. Procedures

Comment: Two respondents noted that DFARS 204.7403 in the proposed rule references procedures at PGI 204.74 that were not published with the proposed rule.

Response: The ''procedures'' section is not included in the final rule. For future reference, when there is PGI associated with a proposed rule, it is available at *https://www.acq.osd.mil/dpap/dars/* under ''Publication Notices''.

18. Contract Clauses (204.7404 Redesignated 204.7303)

Comment: Several respondents recommended making changes to the DFARS clause prescriptions. Two respondents stated that use of ''will potentially have unclassified DoD information'' is vague and will result in usage errors. Two respondents recommended an exemption for fundamental research contracts; two others recommended an exemption for small businesses. One respondent stated that it is not clear if the use of 252.204–70YY negates the need for 252.204–70XX.

Response: The purpose of this rule is to protect the noted category of

unclassified information, as evidenced by inclusion whenever such information would potentially be present; the best means of addressing the identified potential for usage errors is to include the clause in all contracts. The clause at DFARS 252.204–7012 is now prescribed to go in all contracts and solicitations and the additional safeguarding measures will only apply when unclassified controlled technical information is present. This change does not affect the burden placed on contractors to identify which information must be protected. The contractor's size classification is not a sufficient reason to allow a contractor to fail to protect technical information as required by clause DFARS 252.204–7012. The basic clause previously at DFARS 252.204–70XX has been removed and will be handled as a FAR rule under FAR case 2011–020. The clause previously referred to in the proposed rule as 252.204–70YY, Enhanced Safeguarding of Unclassified DoD Information, is now at DFARS 252.204–7012. Use of this clause will not negate the use of any other clauses.

19. Clarify the Disclosure of Information Clause (252.204–7000)

Comment: A number of respondents submitted comments regarding the proposed changes to clause 252.204–7000, Disclosure of Information.

Response: This final rule does not include any changes to the clause at 252.204–7000, Disclosure of Information.

20. Clarify the Basic Clause (Proposed 252.204–70XX)

Comment: Sixteen respondents commented on concerns with the basic clause ranging from definitions, lack of specificity, and implementation issues to scope and cost burden.

Response: The basic clause, at 252.204–70XX in the proposed rule, is not included in this final rule. A basic safeguarding requirement is being developed in FAR case 2011–020.

21. Clarify the Enhanced Clause Definitions

Comment: Eight respondents commented that the definitions for ''information technology,'' ''DoD information systems,'' ''incident,'' ''intrusion,'' ''voice information,'' ''DoD information,'' ''non-public information,'' ''adequate security,'' and ''critical program information'' are too broad.

Response: Many of the definitions used in this document are from DoD standards or regulations. The definitions for ''critical program information'', ''DoD information'', ''incident'', ''intrusion'' and ''nonpublic information'' were removed as they were no longer necessary due to other revisions. The term ''adequate security'' is revised for clarity and consistency.

22. Safeguarding Requirements and Procedures

Comment: Four respondents requested clarification on whether DoD is requiring contractors to perform and document a specific analysis to determine if additional controls are reasonably required, or is just reconfirming that the safeguarding standards may be augmented with additional controls. They also requested clarification regarding whether a formal risk assessment is warranted by this provision, and if so, whether it will be a qualitative assessment (OCTAVE) or quantitative assessment (NIST SP–800–30). There is concern as to whether the risk assessment and proposed enhanced security measures of one contractor will be shared with other contractors or those within the Defense Industrial Base Working Group.

Response: The rule does not require a specific analysis to determine if additional controls are required. The intent is to require that if the contractor is aware, based on an already assessed risk or vulnerability that the specified controls are inadequate, then the contractor must implement additional controls to mitigate the specific shortcoming.

Comment: A respondent questioned the provision that requires contractors with systems that do not meet the specified controls in the table to prepare a written determination that explains why the control(s) is not necessary, but only to provide the written determination to the contracting officer upon request, and suggested wording to be changed to require the determination to be included as part of their proposal.

Response: The rule has been revised to require a written explanation when the contractor intends to deviate from the specified controls. Alternative or superior safeguarding controls will not be considered as a source selection criteria.

23. DoD Information Requiring Enhanced Safeguarding

Comment: Respondents stated that enhanced safeguards would need to be applied to all systems. Comments also indicated that DFARS should not apply to International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR) and information ''bearing current and prior designations indicating controlled access and dissemination.'' ITAR and EAR are regulated by Departments of State and Commerce; other categories of information in the DFARS are already protected by other regulations. ''Critical Program Information'' is poorly defined.

Response: The rule has been revised so the safeguarding requirements only apply to systems that have unclassified controlled technical information resident on or transiting through them. The rule has also been revised to specify that contractors must protect controlled technical information. Additionally, the rule ensures that there are no conflicts with existing regulations. The term ''critical program information'' was not included in the final rule.

Comment: A respondent noted a person communicating information requiring enhanced safeguarding would need to ensure that the recipient of that information also had a system with enhanced safeguarding, which would be challenging.

Response: The contractor has an obligation to ensure that any recipient of information requiring enhanced safeguarding is authorized to receive the information, and that it be transferred with the appropriate security. It is the responsibility of the authorized recipient to safeguard that information appropriately subject to contractual requirements.

24. Enhanced Safeguarding Requirements

Comment: The safeguarding controls must flow down to each subcontractor. All systems in the network would be required to meet enhanced safeguarding, increasing costs. Clarify that enhanced safeguarding only applies to systems where DoD information resides.

Response: The enhanced safeguarding requirement only applies to systems that may have unclassified controlled technical information resident on or transiting through them.

Comment: Several respondents noted the effort and resources required of a security program that is NIST SP 800–53 compliant and the imposition of controls that are not risk based. The respondents requested that DoD consider the financial burden of applying such a security infrastructure that is more appropriate to classified than unclassified information or to more than DoD information.

Response: The rule does not require adoption of a NIST compliant security program. The rule uses the NIST SP 800–53 catalog of security controls as a reference to describe the specific security capabilities that a contractor's system should provide for enhanced safeguarding. The rule has been

modified to apply only to specified controlled technical information.

Comment: A respondent recommended substantial expansion of the NIST controls listed in the table.

Response: The substantial increase in specified controls is not warranted for the sensitivity of the information being protected. Additional controls can be added to any contract when the additional security is required, but broadly applying these additional controls is not justified or practical.

Comment: A respondent noted that the enhanced safeguarding provisions appear to expand export controls and preclude use of the fundamental research exclusion.

Response: The rule does not expand export controls and does not imply any restriction on fundamental research exclusions.

Comment: A respondent noted that there is no explicit statement that this same level of safeguarding is required for subcontractors and recommends the rule specify that the prime contractor flow down the same safeguarding requirement to each level of subcontractor.

Response: Under 252.204–7012 (g) the prime contractor is required to include the substance of this clause in all subcontracts, and each subcontractor must flow the clause down to the next tier.

Comment: Several respondents stated that the requirements for enhanced safeguarding will require contractors to implement a Common Access Card (CAC)-like public key infrastructure (PKI) system on their unclassified networks, citing NIST 800–53 controls AU–10(5) and SC–13(4), or the requirement requiring use of DoD-approved identity authentication credentials for authentication to DoD information systems.

Response: There is no requirement for contractors to implement a PKI system on their unclassified networks processing DoD information. The NIST controls cited merely require that when using cryptography that the cryptographic algorithm meets NIST Federal Information Processing standards, or note that digital signatures can be used to ensure non-repudiation. None of the controls require PKI. If a contractor desires access to a DoD information system (one operated by or on behalf of DoD), then the authentication credentials must meet DoD standards, which typically requires a DoD-approved PKI certificate. This has been a long-standing requirement, but does not imply that the contractor system must implement PKI.

Comment: A respondent noted that the supplementary information section of the proposed rule mentions encryption of data at rest, yet the cited NIST 800–53 for protection of data at rest (SC–28) does not require encryption.

Response: The background information has been aligned in the final rule.

Comment: A respondent recommends requiring compliance with FISMA to ensure that other important FISMA requirements are met.

Response: FISMA applies only to Federal Government information and information systems or systems (or information operated or maintained by contractors on the Government's behalf). FISMA does not does not apply to the contractor information systems addressed under this rule.

Comment: A respondent comments that the rule does not establish a clear link between the sensitivity of the information and the required level of identity assurance and suggests a set of categories for identity assurance that should be incorporated into the rule.

Response: Based on information covered by the rule, the level of identity assurance (AC or Access Control controls) specified in the clause are considered the minimum requirements.

Comment: A respondent notes that Defense Security Service requires that companies under a Foreign Ownership, Control, or Influence (FOCI)-mitigation agreement comply with certain NIST SP 800–53 requirements, the majority of which are required under this rule, leading to confusion, redundancy and wasted resources.

Response: If a company is already compliant with the NIST 800–53 controls for systems that may have unclassified controlled technical information resident on or transiting through them, then they will meet the requirements of this rule.

Comment: A respondent notes that the proposed rule is silent on prohibiting access to non-US persons, and questions whether companies (particularly those with a FOCI mitigation plan) can assume that foreign nationals and entities with a business need to know may access unclassified information unless otherwise subject to export control laws or expressly prohibited by the Government agency.

Response: This rule has no impact on existing information sharing restrictions.

25. Other Requirements

Comment: One respondent was concerned about conflicting obligations under provisions of the proposed rule and recommended that participants in the Defense Industrial Base (DIB) Cyber security/information assurance (CS/IA) program be exempt from complying with the proposed rule in order to prevent the imposition of conflicting obligations.

Response: The final rule and the DIB CS/IA program Framework Agreement are mutually supportive means for safeguarding DoD information on DIB unclassified information systems. The DIB CS/IA program is voluntary and is executed under a bilateral agreement between an eligible DIB company and DoD. The DFARS language establishes contractor requirements executed under a DoD contract.

26. Cyber Incident Reporting

Comment: Eleven respondents commented on the requirement to report incidents within 72 hours of detection. In addition, the DFARS requires indefinite retention of forensics data for the Government and the criteria for damage assessments are broad and unclear. The respondents would like to review and comment on report content or forms prior to publication and suggested that DoD look at DSS NISPOM reporting as an option/model.

Response: The rule has been revised to clarify the reporting requirements and the timeframe for retaining data (90 days) of the potentially compromised data to support a damage assessment if the Government chooses to perform one.

27. Protection of Reported Information

Comment: One respondent requests the Government address how contractor incident reporting information will be protected and how it will be used. The respondent also proposed that the sharing of files and images be voluntary as it is in the Framework Agreement.

Response: Retaining files and images is an important element of the damage assessment process and is required by this rule. DoD will protect incident reporting information and any files or images in accordance with applicable statutes and regulations.

28. Third Party Information

Comment: Two respondents are concerned about exposure of third-party information in data provided by companies to the Government. One respondent recommended the deletion of the following: ''Absent written permission, the third-party information owner may have the right to pursue legal action against the Contractor (or its subcontractors) with access to the nonpublic information for breach or unauthorized disclosure.''

Response: The third party information subparagraph has been removed because support contractors working for the DoD are required to sign non-disclosure agreements. DoD personnel are bound by regulation and statute to protect proprietary information and information furnished in confidence.

29. Subcontracts

Comment: Three respondents note that the proposed rule requires the DFARS to apply to all subcontractors that may potentially have DoD information. In addition, notifications are required through the prime contractor. Potential issues exist with proprietary information and unauthorized disclosure of third party information.

Response: The rule requires that prime contractors report when unclassified controlled technical information has potentially been compromised regardless of whether the incident occurred on a prime contractor's information system or on a subcontractor's information system.

30. Provide a Safe Harbor for Reported Incidents

Comment: One respondent suggested that the rule provide explicit safe harbor in the event of a reported incident.

Response: The rule states in DFARS 204.7302(b)(2) that ''A cyber incident that is properly reported by the contractor shall not, by itself, be interpreted under this clause as evidence that the contractor has failed to provide adequate information safeguards . . .'' The Government does not intend to provide any safe harbor statements.

31. Paperwork Burden

Comment: A number of respondents stated in various qualitative terms that the costs of compliance with the rule would be too large.

Response: The controls in the rule are taken from NIST 800–53 which closely parallels the ISO 27002 standard. As such, the controls represent mainstream industry practices. While there is cost associated with implementing information assurance controls, the use of industry practices provides assurance the costs are reasonable.

Comment: Some respondents opined that few small businesses have the basic infrastructure in place to comply and that implementation of controls would represent a larger percentage of overhead for small businesses than for large.

Response: The contractor's size classification is not a sufficient reason to allow a contractor to fail to protect technical information as required by clause 252.204–7012. The contractor at a minimum must institute the NIST (SP) 800–53 security controls identified in the table at 252.204–7012. If a control is not implemented, the contractor shall submit to the contracting officer a written explanation of how the required security control identified in the table at 252.204–7012 is not applicable, or how an alternative control or protective measure is used to achieve equivalent protection.

Comment: Some respondents stated that the value of controls cannot be measured and that the benefits will not offset the costs.

Response: The purpose of the rule is to reduce the compromise of information. It is difficult to put a price on information and it is generally not calculated in any information protection regime. The benefits of particular controls are also difficult to quantify and further complicated by the 'arms race' dynamic of information protection. It is not possible to determine the exact point at which benefits equal costs. Nevertheless, that does not preclude taking action to protect information and accrue the associated costs.

Comment: One respondent provided an incident reporting rate of approximately 70 reports per company per year, with each report taking approximately 5 hours of company time to complete. This is in contrast to the proposed rule estimate of 0.5 incidents per company per year with a 1 hour burden per response.

Response: Since the burden estimates were estimated for the proposed rule, more data has become available, in particular from voluntary reporting by defense industrial base companies to the Defense Cyber Crime Center. Data from this voluntary program suggests five reports per company per year with a 3.5 hour burden per response. Accordingly, DoD is revising its estimate upward to five reports per company per year with a 3.5 hour burden per response.

Comment: One respondent provided a cost estimate for an appliance to capture images of auditable events of $25,000.

Response: To lower the cost of data collection in the revised rule, DoD must request the data within 90 days. Without this request, there is no obligation to retain data beyond 90 days. Image capture equates to copying the hard drive of an affected machine. The cost of media with sufficient capability to capture a hard drive image of an affected machine is in the range of $100. Assuming an average across all businesses of 12 incidents per year affecting an average of one machine and a 90 day retention period results in the ability to capture and store 3 images. 3 × $100 = $300.

32. Regulatory Flexibility Analysis

Comment: Several respondents stated that this rule will be financially burdensome for small businesses to the point that they will not be able to participate. Two respondents stated that the numbers used in the Initial Regulatory Flexibility Analysis grossly underestimate the number of businesses the rule will affect and the cost as a percentage of revenue that will be required to meet the requirements of the new rule. One respondent suggested that a gradually phased-in approach to implement these safeguards would ease the significant financial burden they impose.

Response: This final rule was drafted with the aim of minimizing the burden of compliance on contractors while implementing the necessary safeguarding requirements.

33. Need for a Public Meeting

Comment: Several respondents suggested that DoD further engage the industry stakeholders, including a suggestion to schedule a public meeting to discuss the rule.

Response: Another public meeting will be considered prior to any future rules dealing with the safeguarding of information.

34. Drafting Recommendations

Comment: One respondent recommends changing all instances of ''unclassified Government information'' to ''DoD information''. Several respondents submitted lists of typos and errors in the proposed rule **Federal Register** notice.

Response: These comments have been taken into account when drafting this final rule. The final rule uses the term ''unclassified controlled technical information.''

35. Out of Scope

Comment: Three respondents made comments that had no relation to the subject rule.

C. Other Changes

The final rule adds a new subpart at 204.73, Safeguarding Unclassified Controlled Technical Information, to conform to the current DFARS baseline. The proposed rule had anticipated adding the new subpart at 204.74.

III. Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is

necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This is a significant regulatory action and, therefore, was subject to review under section 6(b) of E.O. 12866, Regulatory Planning and Review, dated September 30, 1993. This rule is not a major rule under 5 U.S.C. 804.

IV. Regulatory Flexibility Act

A final regulatory flexibility analysis has been prepared consistent with the Regulatory Flexibility Act, 5 U.S.C. 601, *et seq.,* and is summarized as follows:

The objective of this rule is for DoD to avoid compromise of unclassified computer networks on which DoD controlled technical information is resident on or transiting through contractor information systems, and to prevent the exfiltration of controlled technical information on such systems. The benefit of tracking and reporting DoD information compromises is to—

- Assess the impact of compromise;
- Facilitate information sharing and collaboration; and
- Standardize procedures for tracking and reporting compromise of information.

Several respondents stated that this rule will be financially burdensome for small businesses, two respondents stated that the numbers used in the Initial Regulatory Flexibility Analysis grossly underestimate the number of businesses the rule will affect and the cost as a percentage of revenue that will be required to meet the requirements of the new rule, and one respondent suggested that a gradually phased-in approach to implement these safeguards would ease the significant financial burden they impose.

No changes were made to the final rule as a result of these comments. The estimated burden in the final regulatory flexibility analysis has been reduced because the scope of the rule was modified to reduce the categories of information covered and only addresses safeguarding requirements that cover the unclassified controlled technical information and reporting the compromise of unclassified controlled technical information. The final rule is drafted with the aim of minimizing the burden of compliance on contractors while implementing the necessary safeguarding requirements.

This final rule requires information assurance planning, including reporting of information compromise for DoD contractors that handle DoD unclassified controlled technical information. This requirement flows down to subcontracts. DoD believes that most information passed down the supply chain will not require special handling and recognizes that most large contractors handling sensitive information already have sophisticated information assurance programs and can take credit for existing controls with minimal additional cost. However, most small businesses have less sophisticated programs and will realize costs meeting the additional requirements.

Based on figures from the Defense Technical Information Center it is estimated that 6,555 contractors would be handling unclassified controlled technical information and therefore affected by this rule. Of the 6,555 contractors it is estimated that less than half of them are small entities. For the affected small entities a reasonable rule of thumb is that information technology security costs are approximately 0.5% of total revenues. Because there are economies of scale when it comes to information security, larger businesses generally pay only a fraction of that amount.

V. Paperwork Reduction Act

The rule contains information collection requirements that require the approval of the Office of Management and Budget under the Paperwork Reduction Act (44 U.S.C. chapter 35). OMB has cleared this information collection under OMB Control Number 0704–0478, titled: Defense Federal Acquisition Regulation Supplement; Safeguarding Unclassified Controlled Technical Information.

List of Subjects in 48 CFR Parts 204, 212 and 252

Government procurement.

Manuel Quinones,

Editor, Defense Acquisition Regulations System.

Therefore, 48 CFR parts 204, 212, and 252 are amended as follows:

■ 1. The authority citation for 48 CFR parts 204, 212, and 252 continues to read as follows:

Authority: 41 U.S.C. 1303 and 48 CFR Chapter 1.

PART 204—ADMINISTRATIVE MATTERS

■ 2. Add subpart 204.73 to read as follows:

Subpart 204.73—Safeguarding Unclassified Controlled Technical Information

Sec.

Subpart 204.73—Safeguarding Unclassified Controlled Technical Information

204.7300 Scope.

(a) This subpart applies to contracts and subcontracts requiring safeguarding of unclassified controlled technical information resident on or transiting through contractor unclassified information systems.

(b) This subpart does not abrogate any existing contractor physical, personnel, or general administrative security operations governing the protection of unclassified DoD information, nor does it impact requirements of the National Industrial Security Program.

204.7301 Definitions.

As used in this subpart—

Adequate security means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

Controlled technical information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information is to be marked with one of the distribution statements B through F, in accordance with DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

Cyber incident means 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.

Technical information means technical data or computer software, as those terms are defined in the clause at DFARS 252.227–7013, Rights in Technical Data—Non Commercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and

computer software executable code and source code.

204.7302 Policy.

(a) DoD and its contractors and subcontractors will provide adequate security to safeguard unclassified controlled technical information on their unclassified information systems from unauthorized access and disclosure.

(b) When safeguarding is applied to controlled technical information resident on or transiting contractor unclassified information systems—

(1) Contractors must report to DoD certain cyber incidents that affect unclassified controlled technical information resident on or transiting contractor unclassified information systems. Detailed reporting criteria and requirements are set forth in the clause at 252.204–7012, Safeguarding of Unclassified Controlled Technical Information.

(2) A cyber incident that is properly reported by the contractor shall not, by itself, be interpreted under this clause as evidence that the contractor has failed to provide adequate information safeguards for unclassified controlled technical information, or has otherwise failed to meet the requirements of the clause at 252.204–7012. When a cyber incident is reported, the contracting officer shall consult with a security manager of the requiring activity prior to assessing contractor compliance. The contracting officer shall consider such cyber incidents in the context of an overall assessment of the contractor's compliance with the requirements of the clause at 252.204–7012.

204.7303 Contract clause.

Use the clause at 252.204–7012, Safeguarding of Unclassified Controlled Technical Information, in all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items.

PART 212—ACQUISITION OF COMMERCIAL ITEMS

■ 3. Section 212.301 is amended by—

■ a. Redesignating paragraphs (f)(vi) through (lxvii) as (vii) through (lxviii); and

■ b. Adding new paragraph (f)(vi) to read as follows:

212.301 Solicitation provisions and contract clauses for the acquisition of commercial items.

(f) * * *

(vi) Use the clause at 252.204–7012, Safeguarding of Unclassified Controlled Technical Information, as prescribed in 204.7303.

* * * * *

PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

■ 4. Add section 252.204–7012 to read as follows:

252.204–7012 Safeguarding of unclassified controlled technical information.

As prescribed in 204.7303, use the following clause: SAFEGUARDING OF UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION (NOV 2013)

(a) *Definitions.* As used in this clause—

Adequate security means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

Attribution information means information that identifies the Contractor, whether directly or indirectly, by the grouping of information that can be traced back to the Contractor (e.g., program description or facility locations).

Compromise means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

Contractor information system means an information system belonging to, or operated by or for, the Contractor.

Controlled technical information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information is to be marked with one of the distribution statements B-through-F, in accordance with DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

Cyber incident means 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.

Exfiltration means any unauthorized release of data from within an information system. This includes copying the data through covert network channels or the copying of data to unauthorized media.

Media means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which information is recorded, stored, or printed within an information system.

Technical information means technical data or computer software, as those terms are defined in the clause at DFARS 252.227–7013, Rights in Technical Data—Non Commercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) *Safeguarding requirements and procedures for unclassified controlled technical information.* The Contractor shall provide adequate security to safeguard unclassified controlled technical information from compromise. To provide adequate security, the Contractor shall—

(1) Implement information systems security in its project, enterprise, or company-wide unclassified information technology system(s) that may have unclassified controlled technical information resident on or transiting through them. The information systems security program shall implement, at a minimum—

(i) The specified National Institute of Standards and Technology (NIST) Special Publication (SP) 800–53 security controls identified in the following table; or

(ii) If a NIST control is not implemented, the Contractor shall submit to the Contracting Officer a written explanation of how—

(A) The required security control identified in the following table is not applicable; or

(B) An alternative control or protective measure is used to achieve equivalent protection.

(2) Apply other information systems security requirements when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

Table 1—Minimum Security Controls for Safeguarding

Minimum required security controls for unclassified controlled technical information requiring safeguarding in accordance with paragraph (d) of this clause. (A description of the security controls is in the NIST SP 800–53, ''Security and Privacy Controls for Federal Information Systems and Organizations'' (*http://csrc.nist.gov/publications/PubsSPs.html*).)

BILLING CODE 5001–06–P

Access Control	Audit & Accountability	Identification and Authentication	Media Protection	System & Comm Protection
AC-2	AU-2	IA-2	MP-4	SC-2
AC-3(4)	AU-3	IA-4	MP-6	SC-4
AC-4	AU-6(1)	IA-5(1)		SC-7
			Physical and Environmental Protection	
AC-6	AU-7			SC-8(1)
		Incident Response		
AC-7	AU-8		PE-2	SC-13
AC-11(1)	AU-9	IR-2	PE-3	
AC-17(2)		IR-4	PE-5	SC-15
	Configuration Management			
AC-18(1)		IR-5		SC-28
			Program Management	
AC-19	CM-2	IR-6		
				System & Information Integrity
AC-20(1)	CM-6		PM-10	
AC-20(2)	CM-7	Maintenance		SI-2
AC-22	CM-8	MA-4(6)	Risk Assessment	SI-3
		MA-5	RA-5	SI-4
Awareness & Training	Contingency Planning			
AT-2	CP-9	MA-6		

BILLING CODE 5001–06–C

Legend:

AC: Access Control
AT: Awareness and Training MP:
AU: Auditing and Accountability
CM: Configuration Management
CP: Contingency Planning
IA: Identification and Authentication
IR: Incident Response
MA: Maintenance
MP: Media Protection
PE: Physical & Environmental Protection
PM: Program Management
RA: Risk Assessment
SC: System & Communications Protection
SI: System & Information Integrity

(c) *Other requirements.* This clause does not relieve the Contractor of the requirements specified by applicable statutes or other Federal and DoD safeguarding requirements for Controlled Unclassified Information as established by Executive Order 13556, as well as regulations and guidance established pursuant thereto.

(d) *Cyber incident and compromise reporting.*

(1) *Reporting requirement.* The Contractor shall report as much of the following information as can be obtained to the Department of Defense via (*http://dibnet.dod.mil/*) within 72 hours of discovery of any cyber incident, as described in paragraph (d)(2) of this clause, that affects unclassified controlled technical information resident on or transiting through the Contractor's unclassified information systems:

(i) Data Universal Numbering System (DUNS).

(ii) Contract numbers affected unless all contracts by the company are affected.

(iii) Facility CAGE code if the location of the event is different than the prime Contractor location.

(iv) Point of contact if different than the POC recorded in the System for Award Management (address, position, telephone, email).

(v) Contracting Officer point of contact (address, position, telephone, email).

(vi) Contract clearance level.

(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network.

(viii) DoD programs, platforms or systems involved.

(ix) Location(s) of compromise.

(x) Date incident discovered.

(xi) Type of compromise (e.g., unauthorized access, inadvertent release, other).

(xii) Description of technical information compromised.

(xiii) Any additional information relevant to the information compromise.

(2) *Reportable cyber incidents.* Reportable cyber incidents include the following:

(i) A cyber incident involving possible exfiltration, manipulation, or other loss or compromise of any unclassified controlled technical information resident on or transiting through Contractor's, or its subcontractors', unclassified information systems.

(ii) Any other activities not included in paragraph (d)(2)(i) of this clause that allow unauthorized access to the Contractor's unclassified information system on which unclassified controlled technical information is resident on or transiting.

(3) *Other reporting requirements.* This reporting in no way abrogates the Contractor's responsibility for additional safeguarding and cyber incident reporting requirements pertaining to its unclassified information systems under other clauses that may apply to its contract, or as a result of other U.S. Government legislative and regulatory requirements that may apply (e.g., as cited in paragraph (c) of this clause).

(4) *Contractor actions to support DoD damage assessment.* In response to the reported cyber incident, the Contractor shall—

(i) Conduct further review of its unclassified network for evidence of compromise resulting from a cyber incident to include, but is not limited to, identifying compromised computers, servers, specific data and users accounts. This includes analyzing information systems that were part of the compromise, as well as other information systems on the network that were accessed as a result of the compromise;

(ii) Review the data accessed during the cyber incident to identify specific unclassified controlled technical information associated with DoD programs, systems or contracts, including military programs, systems and technology; and

(iii) Preserve and protect images of known affected information systems and all relevant monitoring/packet capture data for at least 90 days from the cyber incident to allow DoD to request information or decline interest.

(5) *DoD damage assessment activities.* If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor point of contact identified in the incident report at (d)(1) of this clause provide all of the damage assessment information gathered in accordance with paragraph (d)(4) of this clause. The Contractor shall comply with damage assessment information requests. The requirement to share files and images exists unless there are legal restrictions that limit a company's ability to share digital media. The Contractor shall inform the Contracting Officer of the source, nature, and prescription of such limitations and the authority responsible.

(e) *Protection of reported information.* Except to the extent that such information is lawfully publicly available without restrictions, the Government will protect information reported or otherwise provided to DoD under this clause in accordance with applicable statutes, regulations, and policies. The Contractor shall identify and mark attribution information reported or otherwise provided to the DoD. The Government may use information, including attribution information and disclose it only to authorized persons for purposes and activities consistent with this clause.

(f) Nothing in this clause limits the Government's ability to conduct law enforcement or counterintelligence activities, or other lawful activities in the interest of homeland security and national security. The results of the activities described in this clause may be used to support an investigation and prosecution of any person or entity, including those attempting to infiltrate or compromise information on a contractor information system in violation of any statute.

(g) *Subcontracts.* The Contractor shall include the substance of this clause, including this paragraph (g), in all subcontracts, including subcontracts for commercial items.

(End of clause)

[FR Doc. 2013–27313 Filed 11–15–13; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Defense Acquisition Regulations System

48 CFR Parts 225 and 252

RIN 0750–AI12

Defense Federal Acquisition Regulation Supplement: Removal of DFARS Coverage on Contractors Performing Private Security Functions (DFARS Case 2013–D037)

AGENCY: Defense Acquisition Regulations System, Department of Defense (DoD).

ACTION: Final rule.

FDIC Document	Hours per response	Number of respondents	Burden hours
Declaration for Government Deposit, Form 7200/04	0.50	30	15
Declaration for Revocable Trust, Form 7200/05	0.50	150	75
Declaration of Independent Activity, Form 7200/06	0.50	5	2.5
Declaration of Independent Activity for Unincorporated Association, Form 7200/07	0.50	5	2.5
Declaration for Joint Ownership Deposit, Form 7200/08	0.50	5	2.5
Declaration for Testamentary Deposit, Form 7200/09	0.50	50	25
Declaration for Defined Contribution Plan, Form 7200/10	1.0	10	10
Declaration for IRA/KEOGH Deposit, Form 7200/11	0.50	5	2.5
Declaration for Defined Benefit Plan, Form 7200/12	1.0	10	10
Declaration of Custodian Deposit, Form 7200/13	0.50	5	2.5
Declaration for Health and Welfare Plan, Form 7200/14	1.0	20	20
Declaration for Plan and Trust, Form 7200/15	0.50	20	10
Declaration for Irrevocable Trust, Form 7200/18	0.50	10	5
Sub-total	.....	5025	182.5
Additional Burden for Deposit Brokers Only	.....	70	137
Total	.....	5095	319.5

General Description of Collection: The collection involves forms used by the FDIC to obtain information from individual depositors and deposit brokers necessary to supplement the records of failed depository institutions to make determinations regarding deposit insurance coverage for depositors of failed institutions. The information provided allows the FDIC to identify the actual owners of an account and each owner's interest in the account.

Request for Comment

Comments are invited on: (a) Whether these collections of information are necessary for the proper performance of the FDIC's functions, including whether the information has practical utility; (b) the accuracy of the estimate of the burden of the information collection, including the validity of the methodology and assumptions used; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the information collection on respondents, including through the use of automated collection techniques or other forms of information technology. All comments will become a matter of public record.

Dated at Washington, DC, this 7th day of May, 2013.

Federal Deposit Insurance Corporation.

Robert E. Feldman,

Executive Secretary.

[FR Doc. 2013–11205 Filed 5–10–13; 8:45 am]

BILLING CODE 6714–01–P

FEDERAL RESERVE SYSTEM

Formations of, Acquisitions by, and Mergers of Bank Holding Companies

The companies listed in this notice have applied to the Board for approval, pursuant to the Bank Holding Company Act of 1956 (12 U.S.C. 1841 *et seq.*) (BHC Act), Regulation Y (12 CFR part 225), and all other applicable statutes and regulations to become a bank holding company and/or to acquire the assets or the ownership of, control of, or the power to vote shares of a bank or bank holding company and all of the banks and nonbanking companies owned by the bank holding company, including the companies listed below.

The applications listed below, as well as other related filings required by the Board, are available for immediate inspection at the Federal Reserve Bank indicated. The applications will also be available for inspection at the offices of the Board of Governors. Interested persons may express their views in writing on the standards enumerated in the BHC Act (12 U.S.C. 1842(c)). If the proposal also involves the acquisition of a nonbanking company, the review also includes whether the acquisition of the nonbanking company complies with the standards in section 4 of the BHC Act (12 U.S.C. 1843). Unless otherwise noted, nonbanking activities will be conducted throughout the United States.

Unless otherwise noted, comments regarding each of these applications must be received at the Reserve Bank indicated or the offices of the Board of Governors not later than June 7, 2013.

A. Federal Reserve Bank of St. Louis (Yvonne Sparks, Community Development Officer) P.O. Box 442, St. Louis, Missouri 63166–2034:

1. *Wildcat Bancshares, Inc.,* Springfield, Missouri; to become a bank holding company by acquiring 100 percent of the voting shares of CBR Bancshares, Corporation, and thereby acquire Citizens Bank of Rogersville, both in Rogersville, Missouri.

Board of Governors of the Federal Reserve System, May 8, 2013.

Michael J. Lewandowski,

Assistant Secretary of the Board.

[FR Doc. 2013–11248 Filed 5–10–13; 8:45 am]

BILLING CODE 6210–01–P

GENERAL SERVICES ADMINISTRATION

[Notice–OERR–2013–01; Docket No. 2013–0002; Sequence 10]

Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition

AGENCY: Office of Emergency Response and Recovery, U.S. General Services Administration (GSA).

ACTION: Request for information.

SUMMARY: On February 12th, 2013, the President issued the Executive Order for Improving Critical Infrastructure Cybersecurity (Executive Order 13636). In accordance with Section 8(e) of Executive Order 13636, within 120 days, the General Services Administration and the Department of Defense, in consultation with the Department of Homeland Security and the Federal Acquisition Regulation Council, are required to make recommendations on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration and address what steps

can be taken to harmonize, and make consistent, existing procurement requirements related to cybersecurity.

Public outreach is a critically important activity for implementation of the Executive Order. In an effort to obtain broad stakeholder involvement, the General Services Administration and the Department of Defense are publishing this Request for Information (RFI) seeking information that can be used in the Section 8(e) report.

DATES: *Effective date:* Submit comments on or before June 12, 2013.

ADDRESSES: Submit comments in response to Notice–OERR–2013–01 by *any of the following methods:*

- *Regulations.gov: http://www.regulations.gov.* Submit comments via the Federal eRulemaking portal by searching for ''Notice–OERR–2013–01''. Select the link ''Submit a Comment'' that corresponds with ''Notice–OERR–2013–01''. Follow the instructions provided at the ''Submit a Comment'' screen. Please include your name, company name (if any), and ''Notice–OERR–2013–01'' on your attached document.
- *Mail:* General Services Administration, Regulatory Secretariat (MVCB), ATTN: Hada Flowers, 1275 First Street NE., 7th Floor, Washington, DC 20417.

Instructions: Please submit comments only and cite ''Notice-OERR–2013–01'', in all correspondence related to this case. All comments received will be posted without change to *http://www.regulations.gov,* including any personal and/or business confidential information provided.

FOR FURTHER INFORMATION CONTACT: Mr. Emile Monette, U.S. General Services Administration, at *emile.monette@gsa.gov* or 703–605–5470.

SUPPLEMENTARY INFORMATION:

A. Background

On February 12th, 2013, the President issued the Executive Order for Improving Critical Infrastructure Cybersecurity (E.O. 13636) and the Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD–21). In accordance with Section 8(e) of Executive Order 13636 (EO), within 120 days, the General Services Administration and the Department of Defense, in consultation with the Department of Homeland Security and the Federal Acquisition Regulation Council, are required to make recommendations on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration and address what steps can be taken to harmonize, and make consistent, existing procurement requirements related to cybersecurity. Among other things, PPD–21 requires the General Services Administration, in consultation with the Department of Defense and the Department of Homeland Security, to jointly provide and support government-wide contracts for critical infrastructure systems and ensure that such contracts include audit rights for the security and resilience of critical infrastructure.

In order to accomplish the task required by EO Section 8(e), the General Services Administration (GSA) and the Department of Defense (DoD) have formed the ''*Joint Working Group on Improving Cybersecurity and Resilience through Acquisition,''* (Working Group) with GSA as the lead agency. The Working Group is comprised of topic-knowledgeable members selected from the DoD, GSA, the Department of Homeland Security (DHS), the Office of Federal Procurement Policy (OFPP), and the National Institute of Standards and Technology (NIST). The Working Group is coordinating its efforts to obtain input from the stakeholder community, including industry, academia, and federal, state, and local government.

Public outreach is a critically important activity for implementation of the EO and PPD. In an effort to obtain broad stakeholder involvement, the Working Group is publishing this Request for Information (RFI) seeking information that can be used in the Section 8(e) report. To the extent applicable, the Section 8(e) recommendations will also lay the foundation for establishment or identification of the government-wide cybersecurity contracts required by PPD–21.

The Working Group is also directly engaged with the DHS Interagency Task Force (ITF). The ITF has been established to lead implementation of the EO and PPD–21, including, among other things, stakeholder engagement. The ITF has established working groups to accomplish the major deliverables and action items required by the EO and PPD, and this RFI for the Section 8(e) report is one element of the larger outreach efforts underway to address the requirements of the EO and PPD.

The importance of common language cannot be overstated. It is apparent that a common lexicon is one of the critical gaps in harmonizing federal acquisition requirements related to cybersecurity.

Given the limitations of the unsettled definition of the word, for purposes of this RFI, the term ''cybersecurity'' is given a broad meaning that includes information security and related areas, like supply chain risk management, information assurance, and software assurance, as well as other efforts to address threats or vulnerabilities flowing from or enabled by connection to digital infrastructure.

In responding to the questions below, please highlight any applicable distinctions in responses related to classified and unclassified acquisitions.

Feasibility and Federal Acquisition: In general, DoD and GSA seek input about the feasibility of incorporating cybersecurity standards into federal acquisitions.

For example:

1. What is the most feasible method to incorporate cybersecurity-relevant standards in acquisition planning and contract administration? What are the cost and other resource implications for the federal acquisition system stakeholders?
2. How can the federal acquisition system, given its inherent constraints and the current fiscal realities, best use incentives to increase cybersecurity amongst federal contractors and suppliers at all tiers? How can this be accomplished while minimizing barriers to entry to the federal market?
3. What are the implications of imposing a set of cybersecurity baseline standards and implementing an associated accreditation program?
4. How can cybersecurity be improved using standards in acquisition planning and contract administration?
5. What are the greatest challenges in developing a cross-sector standards-based approach cybersecurity risk analysis and mitigation process for the federal acquisition system?
6. What is the appropriate balance between the effectiveness and feasibility of implementing baseline security requirements for all businesses?
7. How can the government increase cybersecurity in federal acquisitions while minimizing barriers to entry?
8. Are there specific categories of acquisitions to which federal cybersecurity standards should (or should not) apply?
9. Beyond the general duty to protect government information in federal contracts, what greater levels of security should be applied to which categories of federal acquisition or sectors of commerce?
10. How can the Federal government change its acquisition practices to ensure the risk owner (typically the end user) makes the critical decisions about that risk throughout the acquisition lifecycle?
11. How do contract type (*e.g.,* firm fixed price, time and materials, cost-

plus, etc.) and source selection method (*e.g.,* lowest price technically acceptable, best value, etc.) affect your organization's cybersecurity risk definition and assessment in federal acquisitions?

12. How would you recommend the government evaluate the risk from companies, products, or services that do not comply with cybersecurity standards?

Commercial Practices: In general, DoD and GSA seek information about commercial procurement practices related to cybersecurity.

For example:

13. To what extent do any commonly used commercial standards fulfill federal requirements for your sector?

14. Is there a widely accepted risk analysis framework that is used within your sector that the federal acquisition community could adapt to help determine which acquisitions should include the requirement to apply cybersecurity standards?

15. Describe your organization's policies and procedures for governing cybersecurity risk. How does senior management communicate and oversee these policies and procedures? How has this affected your organization's procurement activities?

16. Does your organization use ''preferred'' or ''authorized'' suppliers or resellers to address cybersecurity risk? How are the suppliers identified and utilized?

17. What tools are you using to brief cybersecurity risks in procurement to your organization's management?

18. What performance metrics and goals do organizations adopt to ensure their ability to manage cybersecurity risk in procurement and maintain the ability to provide essential services?

19. Is your organization a preferred supplier to any customers that require adherence to cybersecurity standards for procurement? What are the requirements to obtain preferred supplier status with this customer?

20. What procedures or assessments does your organization have in place to vet and approve vendors from the perspective of cybersecurity risk?

21. How does your organization handle and address cybersecurity incidents that occur in procurements? Do you aggregate this information for future use? How do you use it?

22. What mechanisms does your organization have in place for the secure exchange of information and data in procurements?

23. Does your organization have a procurement policy for the disposal for hardware and software?

24. How does your organization address new and emerging threats or risks in procurement for private sector commercial transactions? Is this process the same or different when performing a federal contract? Explain.

25. Within your organization's corporate governance structure, where is cyber risk management located (*e.g.,* CIO, CFO, Risk Executive)?

26. If applicable, does your Corporate Audit/Risk Committee examine retained risks from cyber and implement special controls to mitigate those retained risks?

27. Are losses from cyber risks and breaches treated as a cost of doing business?

28. Does your organization have evidence of a common set of information security standards (*e.g.,* written guidelines, operating manuals, etc)?

29. Does your organization disclose vulnerabilities in your product/services to your customers as soon as they become known? Why or why not?

30. Does your organization have track-and-trace capabilities and/or the means to establish the provenance of products/services throughout your supply chain?

31. What testing and validation practices does your organization currently use to ensure security and reliability of products it purchases?

Harmonization: In general, DoD and GSA seek information about any conflicts in statutes, regulations, policies, practices, contractual terms and conditions, or acquisition processes affecting federal acquisition requirements related to cybersecurity and how the federal government might address those conflicts.

For example:

32. What cybersecurity requirements that affect procurement in the United States (*e.g.,* local, state, federal, and other) has your organization encountered? What are the conflicts in these requirements, if any? How can any such conflicts best be harmonized or de-conflicted?

33. What role, in your organization's view, should national/international standards organizations play in cybersecurity in federal acquisitions?

34. What cybersecurity requirements that affect your organization's procurement activities outside of the United States (*e.g.,* local, state, national, and other) has your organization encountered? What are the conflicts in these requirements, if any? How can any such conflicts best be harmonized or de-conflicted with current or new requirements in the United States?

35. Are you required by the terms of contracts with federal agencies to comply with unnecessarily duplicative or conflicting cybersecurity requirements? Please provide details.

36. What policies, practices, or other acquisition processes should the federal government change in order to achieve cybersecurity in federal acquisitions?

37. Has your organization recognized competing interests amongst procurement security standards in the private sector? How has your company reconciled these competing or conflicting standards?

Dated: May 7, 2013.

Darren Blue,

Associate Administrator for the GSA, Office of Emergency Response and Recovery.

[FR Doc. 2013–11239 Filed 5–10–13; 8:45 am]

BILLING CODE 6820–89–P

GENERAL SERVICES ADMINISTRATION

[FMR Bulletin–PBS–2013–01; Docket 2013–0002; Sequence 5]

Federal Management Regulation; Redesignations of Federal Buildings

AGENCY: Public Buildings Service (PBS), General Services Administration (GSA).

ACTION: Notice of a bulletin.

SUMMARY: The attached bulletin announces the designation and redesignation of six Federal buildings.

DATES: *Expiration Date:* This bulletin announcement expires July 30, 2013. The building designations and redesignations remains in effect until canceled or superseded by another bulletin.

FOR FURTHER INFORMATION CONTACT: U.S. General Services Administration, Public Buildings Service (PBS), 1800 F Street NW., Washington, DC 20405, telephone number: 202–501–1100.

Dan Tangherlini,

Acting Administrator of General Services.

U.S. GENERAL SERVICES ADMINISTRATION

DESIGNATIONS AND REDESIGNATION OF FEDERAL BUILDINGS

TO: Heads of Federal Agencies

SUBJECT: Redesignations of Federal Buildings

1. *What is the purpose of this bulletin*? This bulletin announces the designation and redesignation of six Federal buildings.

2. *When does this bulletin expire*? This bulletin announcement expires July 30, 2013. The building designations and redesignations remain in effect until

Proposed Rules

Federal Register
Vol. 77, No. 165
Friday, August 24, 2012

This section of the FEDERAL REGISTER contains notices to the public of the proposed issuance of rules and regulations. The purpose of these notices is to give interested persons an opportunity to participate in the rule making prior to the adoption of the final rules.

DEPARTMENT OF THE TREASURY

Internal Revenue Service

26 CFR Part 1

[REG–113738–12]

RIN 1545–BK94

Amendment of Prohibited Payment Option Under Single-Employer Defined Benefit Plan of Plan Sponsor in Bankruptcy; Hearing Cancellation

AGENCY: Internal Revenue Service (IRS), Treasury.

ACTION: Cancellation of notice of public hearing on proposed rulemaking.

SUMMARY: This document cancels a public hearing on proposed regulations under section 411(d)(6) of the Internal Revenue Code. The proposed regulations provide guidance under the anti-cutback rules of section 411(d)(6) of the Internal Revenue Code, which generally prohibit plan amendments eliminating or reducing accrued benefits, early retirement benefits, retirement-type subsidies, and optional forms of benefit under qualified retirement plans.

DATES: The public hearing, originally scheduled for August 24, 2012 at 10 a.m. is cancelled.

FOR FURTHER INFORMATION CONTACT: Oluwafunmilayo Taylor of the Publications and Regulations Branch, Legal Processing Division, Associate Chief Counsel (Procedure and Administration) at (202) 622–7180 (not a toll-free number).

SUPPLEMENTARY INFORMATION: A notice of proposed rulemaking and a notice of public hearing that appeared in the **Federal Register** on Thursday, June 21, 2012 (77 FR 37349) announced that a public hearing was scheduled for August 24, 2012, at 10 a.m. in the IRS Auditorium, Internal Revenue Building, 1111 Constitution Avenue NW., Washington, DC. The subject of the public hearing was under the sections 411(d)(6) of the Internal Revenue Code.

The public comment period for these regulations expired on August 16, 2012. The notice of proposed rulemaking and notice of public hearing instructed those interested in testifying at the public hearing to submit a request to speak and an outline of the topics to be addressed. The public hearing scheduled for August 24, 2012, is cancelled.

LaNita VanDyke,

Chief, Publications and Regulations Branch, Legal Processing Division, Associate Chief Counsel, (Procedure and Administration).

[FR Doc. 2012–20995 Filed 8–22–12; 4:15 pm]

BILLING CODE 4830–01–P

DEPARTMENT OF DEFENSE

GENERAL SERVICES ADMINISTRATION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

48 CFR Parts 4, 7, 12, 42, and 52

[FAR Case 2011–020; Docket 2011–0020; Sequence 1]

RIN 9000–AM19

Federal Acquisition Regulation; Basic Safeguarding of Contractor Information Systems

AGENCY: Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA).

ACTION: Proposed rule.

SUMMARY: DoD, GSA, and NASA are proposing to amend the Federal Acquisition Regulation (FAR) to add a new subpart and contract clause for the basic safeguarding of contractor information systems that contain information provided by or generated for the Government (other than public information) that will be resident on or transiting through contractor information systems.

DATES: Interested parties should submit written comments to the Regulatory Secretariat at one of the addressees shown below on or before October 23, 2012 to be considered in the formation of the final rule.

ADDRESSES: Submit comments in response to FAR Case 2011–020 by any of the following methods:

- *Regulations.gov: http://www.regulations.gov.* Submit comments via the Federal eRulemaking portal by searching for ''FAR Case 2011–020.'' Select the link ''Submit a Comment'' that corresponds with ''FAR Case 2011–020.'' Follow the instructions provided at the ''Submit a Comment'' screen. Please include your name, company name (if any), and ''FAR Case 2011–020'' on your attached document.
- *Fax:* 202–501–4067.
- *Mail:* General Services Administration, Regulatory Secretariat (MVCB), ATTN: Hada Flowers, 1275 First Street NE., 7th Floor, Washington, DC 20417.

Instructions: Please submit comments only and cite FAR Case 2011–020, in all correspondence related to this case. All comments received will be posted without change to *http://www.regulations.gov,* including any personal and/or business confidential information provided.

FOR FURTHER INFORMATION CONTACT: Ms. Patricia Corrigan, Procurement Analyst, at 202–208–1963, for clarification of content. For information pertaining to status or publication schedules, contact the Regulatory Secretariat at 202–501–4755. Please cite FAR Case 2011–020.

SUPPLEMENTARY INFORMATION:

I. Background

The FAR presently does not specifically address the safeguarding of contractor information systems that contain or process information provided by or generated for the Government (other than public information). DoD published an Advance Notice of Proposed Rulemaking (ANPR) and notice of public meeting in the **Federal Register** at 75 FR 9563 on March 3, 2010, under Defense Federal Acquisition Regulation Supplement (DFARS) Case 2008–D028, Safeguarding Unclassified Information. The ANPR addressed basic and enhanced safeguarding procedures for the protection of DoD unclassified information. Basic protection measures are first-level information technology security measures used to deter unauthorized disclosure, loss, or compromise. The ANPR also addressed enhanced information protection measures that included requirements for encryption and network intrusion protection.

Resulting public comments of the DFARS rule were considered in drafting a proposed FAR rule under FAR case

2009–030, which focused on the basic safeguarding of unclassified Government information within contractor information systems. The Councils agreed to the draft proposed FAR rule, but it was not published. On June 29, 2011, the contents of FAR case 2009–030 were rolled into FAR case 2011–020, which is not limited to a single category of Government information, *e.g.,* unclassified.

This proposed FAR rule would add a contract clause to address requirements for the basic safeguarding of contractor information systems that contain or process information provided by or generated for the Government (other than public information). DoD, GSA, and NASA concluded that these requirements are an extension of the requirements, under the Federal Information Security Management Act (FISMA) of 2002, for Federal agencies to provide information security for information and information systems that support the operations and assets of the agency, including those managed by contractors. 44 U.S.C. 3544(a)(1)(A)(ii) describes Federal agency security responsibilities as including ''information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.'' The safeguarding measures would not apply to public information as defined at 44 U.S.C. 3502.

II. Proposed Rule

The proposed FAR changes would add a new subpart at 4.17, Basic Safeguarding of Contractor Information Systems. The other FAR changes include the following:

- Definitions at FAR 4.1701, for ''information'' derived from the Committee on National Security Systems Instruction 4009, April 26, 2010, and ''information system'' and ''public information'' from 44 U.S.C. 3502;
- Applicability at FAR 4.1702, which applies the rule to commercial items and commercial-off-the-shelf items when a contractor's information system contains information provided by or generated for the Government (other than public information) that will be resident on or transiting through contractor information systems. It also may be applied under the simplified acquisition threshold when the contracting officer determines that inclusion of the clause is appropriate.
- Applicability added to FAR 12.301, Solicitation provisions and contract clauses for the acquisition of commercial items;
- A clause at FAR 52.204–XX, Basic Safeguarding of Contractor Information Systems, which requires the contractor to provide protective measures to information provided by or generated for the Government (other than public information) that will be resident on or transiting through contractor information systems in the following areas:
  - Public computers or Web sites.
  - Transmitting electronic information.
  - Transmitting voice and fax information.
  - Physical and electronic barriers.
  - Sanitization.
  - Intrusion protection.
  - Transfer limitations.
- Conforming changes were made at FAR subparts 7.1, Acquisition Plans and 42.3, Contract Administration Office Functions.

The proposed FAR changes address only basic requirements for the safeguarding of contractor information systems, and may be altered as necessary to align with any future direction given in response to ongoing efforts led by the National Archives and Records Administration in the implementation of Executive Order 13556 of November 4, 2010, ''Controlled Unclassified Information,'' published in the **Federal Register** at 75 FR 68675, on November 9, 2010. Further, the clause prescribed in the proposed rule is not intended to implement any other, more specific safeguarding requirements, or to conflict with any contract clauses or requirements that specifically address the safeguarding of information or information systems. If any restrictions or authorizations in this clause are inconsistent with a requirement of any other clause in a contract, the requirement of the other clause shall take precedence over the requirement of the clause at FAR 52.204–XX.

There are other pending rules that are related to this rule, but this rule does not duplicate, overlap, or conflict with the other rules. The other FAR rules are as follows:

- FAR Case 2011–001, Organizational Conflict of Interest and Contractor Access to Nonpublic Information; and
- FAR Case 2011–010, Sharing Cyber Threat Information.

The status of DFARS and FAR cases can be tracked at *http://www.acq.osd.mil/dpap/dars/case_status.html.*

II. Executive Order 12866 and 13563

Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This is a significant regulatory action and, therefore, was subject to review under section 6(b) of Executive Order 12866, Regulatory Planning and Review, dated September 30, 1993. This rule is not a major rule under 5 U.S.C. 804.

III. Regulatory Flexibility Act

The change may have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act 5 U.S.C. 601, *et seq.* The Initial Regulatory Flexibility Analysis (IRFA) is summarized as follows:

This action is being implemented to revise the Federal Acquisition Regulation (FAR) to protect against the compromise of contractor computer networks on which information provided by or generated for the Government (other than public information) that will be resident on or transiting through contractor information systems.

The objective of this rule is to improve the protection of information provided by or generated for the Government (other than public information) that will be resident on or transiting through contractor information systems by employing basic security measures, as identified in the clause to appropriately protect information provided by or generated for the Government (other than public information) that will be resident on or transiting through contractor information systems from unauthorized disclosure, loss, or compromise.

This proposed rule applies to all Federal contractors and appropriate subcontractors regardless of size or business ownership. The resultant cost impact is considered not significant, since the first-level protective measures (*i.e.,* updated virus protection, the latest security software patches, etc.) are typically employed as part of the routine course of doing business. It is recognized that the cost of not using basic information technology system protection measures would be a significant detriment to contractor and Government business, resulting in reduced system performance and the potential loss of valuable information. It is also recognized that prudent business practices designed to protect an information technology system are typically a common part of everyday operations. As a result, the benefit of securely receiving and processing information provided by or generated for the Government (other than public information) that will be resident on or transiting through contractor information systems offers substantial value to contractors and the Government by reducing vulnerabilities to contractor systems by keeping information

provided by or generated for the Government (other than public information) that will be resident on or transiting through contractor information systems safe.

There are no known significant alternatives to the rule that would further minimize any economic impact of the rule on small entities.

The Regulatory Secretariat will be submitting a copy of the Initial Regulatory Flexibility Analysis (IRFA) to the Chief Counsel for Advocacy of the Small Business Administration. A copy of the IRFA may be obtained from the Regulatory Secretariat. The Councils invite comments from small business concerns and other interested parties on the expected impact of this rule on small entities.

DoD, GSA, and NASA will also consider comments from small entities concerning the existing regulations in subparts affected by this rule in accordance with 5 U.S.C. 610. Interested parties must submit such comments separately and should cite 5 U.S.C. 610 (FAR Case 2011–020) in correspondence.

IV. Paperwork Reduction Act

The proposed rule does not contain any information collection requirements that require the approval of the Office of Management and Budget under the Paperwork Reduction Act (44 U.S.C. chapter 35).

List of Subjects in 48 CFR Parts 4, 7, 12, 42, and 52

Government procurement.

Dated: August 17, 2012.

Laura Auletta,

Director, Office of Governmentwide Acquisition Policy, Office of Acquisition Policy, Office of Governmentwide Policy.

Therefore, DoD, GSA, and NASA propose amending 48 CFR parts 4, 7, 12, 42, and 52 as set forth below:

1. The authority citation for 48 CFR parts 4, 7, 12, 42, and 52 are revised to read as follows:

Authority: 40 U.S.C. 121(c); 10 U.S.C. chapter 137; and 51 U.S.C. 20113.

PART 4—ADMINISTRATIVE MATTERS

2. Add Subpart 4.17 to read as follows.

Subpart 4.17—Basic Safeguarding of Contractor Information Systems

Sec.

Subpart 4.17—Basic Safeguarding of Contractor Information Systems

4.1700 Scope of subpart.

This subpart prescribes policies and procedures for safeguarding information provided by or generated for the Government (other than public information) that will be resident on or transiting through contractor information systems.

4.1701 Definitions.

As used in this subpart—

Information means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

Public information means any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public (44 U.S.C. 3502).

Safeguarding means measures or controls that are prescribed to protect information.

4.1702 Applicability.

This subpart applies to all solicitations, contracts (including orders and those for commercial items and commercially available off-the-shelf items), when a contractor's information system may contain information provided by or generated for the Government (other than public information).

4.1703 Solicitation provision and contract clause.

Use the clause at 52.204–XX, Basic Safeguarding of Contractor Information Systems, in solicitations and contracts above the simplified acquisition threshold when the contractor or a subcontractor at any tier may have information residing in or transiting through its information system, where such information is provided by or generated for the Government (other than public information). The clause may also be used in contracts below the simplified acquisition threshold when the contracting officer determines that inclusion of the clause is appropriate.

PART 7—ACQUISITION PLANNING

3. Amend section 7.105 by revising paragraph (b)(18) to read as follows.

7.105 Contents of written acquisition plans.

* * * * *

(b) * * *

(18) *Security considerations.*

(i) For acquisitions dealing with classified matters, discuss how adequate security will be established, maintained, and monitored (see subpart 4.4).

(ii) For information technology acquisitions, discuss how agency information security requirements will be met.

(iii) For acquisitions requiring routine contractor physical access to a Federally-controlled facility and/or routine access to a Federally controlled information system, discuss how agency requirements for personal identity verification of contractors will be met (see subpart 4.13).

(iv) For acquisitions that may require information provided by or generated for the Government (other than public information) to reside on or transit through contractor information systems, discuss how this information will be protected (see subpart 4.17).

* * * * *

PART 12—ACQUISITION OF COMMERCIAL ITEMS

4. Amend section 12.301 by redesignating paragraph (d)(2) as paragraph (d)(4), and adding a new paragraph (d)(2) to read as follows:

12.301 Solicitation provisions and contract clauses for the acquisition of commercial items.

* * * * *

(d) * * *

(2) Insert the clause at 52.204–XX, Basic Safeguarding of Contractor Information Systems, in solicitations and contracts, as prescribed in 4.1703.

* * * * *

PART 42—CONTRACT MANAGEMENT

5. Amend section 42.302 by redesignating paragraphs (a)(21) through (a)(71) as paragraphs (a)(22) through (a)(72); and adding a new paragraph (a)(21) to read as follows.

42.302 Contract administration functions.

(a) * * *

(21) Ensure that the contractor has protective measures in place, consistent with the requirements of the clause at 52.204–XX.

* * * * *

PART 52—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

6. Add section 52.204–XX to read as follows:

52.204–XX Basic Safeguarding of Contractor Information Systems.

As prescribed in 4.1703, use the following clause:

Basic Safeguarding of Contractor Information Systems (Date)

(a) *Definitions.* As used in this clause—

Clearing means removal of data from an information system, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities (*i.e.,* through the keyboard); however, the data may be reconstructed using laboratory methods.

Compromise means disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. This includes copying the data through covert network channels or the copying of data to unauthorized media.

Data means a subset of information in an electronic format that allows it to be retrieved or transmitted.

Information means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

Intrusion means an unauthorized act of bypassing the security mechanisms of a system.

Media means physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, large scale integration memory chips, and printouts (but not including display media, *e.g.,* a computer monitor, cathode ray tube (CRT) or other (transient) visual output) onto which information is recorded, stored, or printed within an information system.

Public information means any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public (44 U.S.C. 3502).

Safeguarding means measures or controls that are prescribed to protect information.

Voice means all oral information regardless of transmission protocol.

(b) *Safeguarding requirements and procedures.* The Contractor shall apply the following basic safeguarding requirements to protect information provided by or generated for the Government (other than public information) which resides on or transits through its information systems from unauthorized access and disclosure:

(1) *Protecting information on public computers or Web sites:* Do not process information provided by or generated for the Government (other than public information) on public computers (*e.g.,* those available for use by the general public in kiosks, hotel business centers) or computers that do not have access control. Information provided by or generated for the Government (other than public information) shall not be posted on Web sites that are publicly available or have access limited only by domain/Internet Protocol restriction. Such information may be posted to web pages that control access by user ID/password, user certificates, or other technical means, and that provide protection via use of security technologies. Access control may be provided by the intranet (versus the Web site itself or the application it hosts).

(2) *Transmitting electronic information.* Transmit email, text messages, blogs, and similar communications that contain information provided by or generated for the Government (other than public information), using technology and processes that provide the best level of security and privacy available, given facilities, conditions, and environment.

(3) *Transmitting voice and fax information.* Transmit information provided by or generated for the Government (other than public information), via voice and fax only when the sender has a reasonable assurance that access is limited to authorized recipients.

(4) *Physical and electronic barriers.* Protect information provided by or generated for the Government (other than public information), by at least one physical and one electronic barrier (*e.g.,* locked container or room, login and password) when not under direct individual control.

(5) *Sanitization.* At a minimum, clear information on media that have been used to process information provided by or generated for the Government (other than public information), before external release or disposal. Overwriting is an acceptable means of clearing media in accordance with National Institute of Standards and Technology 800–88, Guidelines for Media Sanitization, at *http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.*

(6) *Intrusion protection.* Provide at a minimum the following protections against computer intrusions and data compromise:

(i) Current and regularly updated malware protection services, *e.g.,* anti-virus, anti-spyware.

(ii) Prompt application of security-relevant software upgrades, *e.g.,* patches, service-packs, and hot fixes.

(7) *Transfer limitations.* Transfer information provided by or generated for the Government (other than public information), only to those subcontractors that both require the information for purposes of contract performance and provide at least the same level of security as specified in this clause.

(c) *Subcontracts.* The Contractor shall include the substance of this clause, including this paragraph (c), in all subcontracts under this contract that may have information residing in or transiting through its information system, where such is provided by or generated for the Government (other than public information).

(d) *Other contractual requirements regarding the safeguarding of information.* This clause addresses basic requirements, and is subordinate to any other contract clauses or requirements that specifically address the safeguarding of information or information systems. If any restrictions or authorizations in this clause are inconsistent with a requirement of any other such clause in this contract, the requirement of the other clause shall take precedence over the requirement of this clause.

[FR Doc. 2012–20881 Filed 8–23–12; 8:45 am]

BILLING CODE 6820–EP–P

DEPARTMENT OF TRANSPORTATION

National Highway Traffic Safety Administration

49 CFR Part 535

[NHTSA 2012–0126]

RIN 2127–AK74

Greenhouse Gas Emissions Standards and Fuel Efficiency Standards for Medium- and Heavy-Duty Engines and Vehicles

AGENCY: National Highway Traffic Safety Administration (NHTSA), DOT.

ACTION: Denial of petition for rulemaking.

SUMMARY: The National Highway Traffic Administration (NHTSA) is denying the petition of Plant Oil Powered Diesel Fuel Systems, Inc. (''POP Diesel'') to amend the final rules establishing fuel efficiency standards for medium- and heavy-duty vehicles. NHTSA does not believe that POP Diesel has set forth a basis for rulemaking. The agency disagrees with the petitioner's assertion that a failure to specifically consider pure vegetable oil, and technology to enable its usage, as a feasible technology in heavy-duty vehicles, led to the adoption of less stringent standards. NHTSA also disagrees with POP's assertion that the agency failed to adequately consider the rebound effect in setting the standards.

FOR FURTHER INFORMATION CONTACT:

For Non-Legal Issues: James Tamm, Office of Rulemaking, National Highway Traffic Safety Administration, 1200 New Jersey Ave. SE., Washington, DC 20590, Telephone (202) 493–0515.

For Legal Issues: Lily Smith, Office of Chief Counsel, National Highway Traffic Safety Administration, 1200 New Jersey Ave. SE., Washington, DC 20590, Telephone: (202) 366–2992.

SUPPLEMENTARY INFORMATION:

I. Background

On September 15, 2011, NHTSA issued a final rule creating fuel efficiency standards for medium- and heavy-duty vehicles (''heavy-duty rule'') (76 FR 57106).

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

FEDERAL REGISTER

Vol. 78 Tuesday,
No. 33 February 19, 2013

Part III

The President

Executive Order 13636—Improving Critical Infrastructure Cybersecurity

Federal Register
Vol. 78, No. 33
Tuesday, February 19, 2013

Presidential Documents

Title 3—

The President

Executive Order 13636 of February 12, 2013

Improving Critical Infrastructure Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Policy.* Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

Sec. 2. *Critical Infrastructure.* As used in this order, the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Sec. 3. *Policy Coordination.* Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive–1 of February 13, 2009 (Organization of the National Security Council System), or any successor.

Sec. 4. *Cybersecurity Information Sharing.* (a) It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the ''Secretary''), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.

(b) The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports produced pursuant to section 4(a) of this order to the targeted entity. Such process shall also, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them. The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a system for tracking the production, dissemination, and disposition of these reports.

(c) To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary, consistent with 6 U.S.C. 143 and in collaboration with the Secretary of

Defense, shall, within 120 days of the date of this order, establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors. This voluntary information sharing program will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure.

(d) The Secretary, as the Executive Agent for the Classified National Security Information Program created under Executive Order 13549 of August 18, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities), shall expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in section 9 of this order.

(e) In order to maximize the utility of cyber threat information sharing with the private sector, the Secretary shall expand the use of programs that bring private sector subject-matter experts into Federal service on a temporary basis. These subject matter experts should provide advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.

Sec. 5. *Privacy and Civil Liberties Protections.* (a) Agencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities.

(b) The Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security (DHS) shall assess the privacy and civil liberties risks of the functions and programs undertaken by DHS as called for in this order and shall recommend to the Secretary ways to minimize or mitigate such risks, in a publicly available report, to be released within 1 year of the date of this order. Senior agency privacy and civil liberties officials for other agencies engaged in activities under this order shall conduct assessments of their agency activities and provide those assessments to DHS for consideration and inclusion in the report. The report shall be reviewed on an annual basis and revised as necessary. The report may contain a classified annex if necessary. Assessments shall include evaluation of activities against the Fair Information Practice Principles and other applicable privacy and civil liberties policies, principles, and frameworks. Agencies shall consider the assessments and recommendations of the report in implementing privacy and civil liberties protections for agency activities.

(c) In producing the report required under subsection (b) of this section, the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of DHS shall consult with the Privacy and Civil Liberties Oversight Board and coordinate with the Office of Management and Budget (OMB).

(d) Information submitted voluntarily in accordance with 6 U.S.C. 133 by private entities under this order shall be protected from disclosure to the fullest extent permitted by law.

Sec. 6. *Consultative Process.* The Secretary shall establish a consultative process to coordinate improvements to the cybersecurity of critical infrastructure. As part of the consultative process, the Secretary shall engage and consider the advice, on matters set forth in this order, of the Critical Infrastructure Partnership Advisory Council; Sector Coordinating Councils; critical infrastructure owners and operators; Sector-Specific Agencies; other relevant agencies; independent regulatory agencies; State, local, territorial, and tribal governments; universities; and outside experts.

Sec. 7. *Baseline Framework to Reduce Cyber Risk to Critical Infrastructure.* (a) The Secretary of Commerce shall direct the Director of the National

Institute of Standards and Technology (the ''Director'') to lead the development of a framework to reduce cyber risks to critical infrastructure (the ''Cybersecurity Framework''). The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible. The Cybersecurity Framework shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Institute of Standards and Technology Act, as amended (15 U.S.C. 271 *et seq.*), the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113), and OMB Circular A–119, as revised.

(b) The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.

(c) The Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties.

(d) In developing the Cybersecurity Framework, the Director shall engage in an open public review and comment process. The Director shall also consult with the Secretary, the National Security Agency, Sector-Specific Agencies and other interested agencies including OMB, owners and operators of critical infrastructure, and other stakeholders through the consultative process established in section 6 of this order. The Secretary, the Director of National Intelligence, and the heads of other relevant agencies shall provide threat and vulnerability information and technical expertise to inform the development of the Cybersecurity Framework. The Secretary shall provide performance goals for the Cybersecurity Framework informed by work under section 9 of this order.

(e) Within 240 days of the date of this order, the Director shall publish a preliminary version of the Cybersecurity Framework (the ''preliminary Framework''). Within 1 year of the date of this order, and after coordination with the Secretary to ensure suitability under section 8 of this order, the Director shall publish a final version of the Cybersecurity Framework (the ''final Framework'').

(f) Consistent with statutory responsibilities, the Director will ensure the Cybersecurity Framework and related guidance is reviewed and updated as necessary, taking into consideration technological changes, changes in cyber risks, operational feedback from owners and operators of critical infrastructure, experience from the implementation of section 8 of this order, and any other relevant factors.

Sec. 8. *Voluntary Critical Infrastructure Cybersecurity Program.* (a) The Secretary, in coordination with Sector-Specific Agencies, shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities (the ''Program'').

(b) Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

(c) Sector-Specific Agencies shall report annually to the President, through the Secretary, on the extent to which owners and operators notified under section 9 of this order are participating in the Program.

(d) The Secretary shall coordinate establishment of a set of incentives designed to promote participation in the Program. Within 120 days of the date of this order, the Secretary and the Secretaries of the Treasury and Commerce each shall make recommendations separately to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, that shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants in the Program.

(e) Within 120 days of the date of this order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary and the Federal Acquisition Regulatory Council, shall make recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. The report shall address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity.

Sec. 9. *Identification of Critical Infrastructure at Greatest Risk.* (a) Within 150 days of the date of this order, the Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. In identifying critical infrastructure for this purpose, the Secretary shall use the consultative process established in section 6 of this order and draw upon the expertise of Sector-Specific Agencies. The Secretary shall apply consistent, objective criteria in identifying such critical infrastructure. The Secretary shall not identify any commercial information technology products or consumer information technology services under this section. The Secretary shall review and update the list of identified critical infrastructure under this section on an annual basis, and provide such list to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs.

(b) Heads of Sector-Specific Agencies and other relevant agencies shall provide the Secretary with information necessary to carry out the responsibilities under this section. The Secretary shall develop a process for other relevant stakeholders to submit information to assist in making the identifications required in subsection (a) of this section.

(c) The Secretary, in coordination with Sector-Specific Agencies, shall confidentially notify owners and operators of critical infrastructure identified under subsection (a) of this section that they have been so identified, and ensure identified owners and operators are provided the basis for the determination. The Secretary shall establish a process through which owners and operators of critical infrastructure may submit relevant information and request reconsideration of identifications under subsection (a) of this section.

Sec. 10. *Adoption of Framework.* (a) Agencies with responsibility for regulating the security of critical infrastructure shall engage in a consultative process with DHS, OMB, and the National Security Staff to review the preliminary Cybersecurity Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks. In making such determination, these agencies shall consider the identification

of critical infrastructure required under section 9 of this order. Within 90 days of the publication of the preliminary Framework, these agencies shall submit a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the Director of OMB, and the Assistant to the President for Economic Affairs, that states whether or not the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure, the existing authorities identified, and any additional authority required.

(b) If current regulatory requirements are deemed to be insufficient, within 90 days of publication of the final Framework, agencies identified in subsection (a) of this section shall propose prioritized, risk-based, efficient, and coordinated actions, consistent with Executive Order 12866 of September 30, 1993 (Regulatory Planning and Review), Executive Order 13563 of January 18, 2011 (Improving Regulation and Regulatory Review), and Executive Order 13609 of May 1, 2012 (Promoting International Regulatory Cooperation), to mitigate cyber risk.

(c) Within 2 years after publication of the final Framework, consistent with Executive Order 13563 and Executive Order 13610 of May 10, 2012 (Identifying and Reducing Regulatory Burdens), agencies identified in subsection (a) of this section shall, in consultation with owners and operators of critical infrastructure, report to OMB on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements. This report shall describe efforts made by agencies, and make recommendations for further actions, to minimize or eliminate such requirements.

(d) The Secretary shall coordinate the provision of technical assistance to agencies identified in subsection (a) of this section on the development of their cybersecurity workforce and programs.

(e) Independent regulatory agencies with responsibility for regulating the security of critical infrastructure are encouraged to engage in a consultative process with the Secretary, relevant Sector-Specific Agencies, and other affected parties to consider prioritized actions to mitigate cyber risks for critical infrastructure consistent with their authorities.

Sec. 11. *Definitions.* (a) ''Agency'' means any authority of the United States that is an ''agency'' under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).

(b) ''Critical Infrastructure Partnership Advisory Council'' means the council established by DHS under 6 U.S.C. 451 to facilitate effective interaction and coordination of critical infrastructure protection activities among the Federal Government; the private sector; and State, local, territorial, and tribal governments.

(c) ''Fair Information Practice Principles'' means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

(d) ''Independent regulatory agency'' has the meaning given the term in 44 U.S.C. 3502(5).

(e) ''Sector Coordinating Council'' means a private sector coordinating council composed of representatives of owners and operators within a particular sector of critical infrastructure established by the National Infrastructure Protection Plan or any successor.

(f) ''Sector-Specific Agency'' has the meaning given the term in Presidential Policy Directive–21 of February 12, 2013 (Critical Infrastructure Security and Resilience), or any successor.

Sec. 12. *General Provisions.* (a) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater

extent than the authority the agency has under existing law. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law.

(b) Nothing in this order shall be construed to impair or otherwise affect the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be interpreted to supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence and law enforcement operations.

(d) This order shall be implemented consistent with U.S. international obligations.

(e) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

THE WHITE HOUSE,
February 12, 2013.

[FR Doc. 2013–03915
Filed 2–15–13; 11:15 am]
Billing code 3295–F3

JAN 2 3 2014

MEMORANDUM FOR ASSISTANT TO THE PRESIDENT FOR HOMELAND SECURITY
ASSISTANT TO THE PRESIDENT FOR ECONOMIC AFFAIRS

SUBJECT: Improving Cybersecurity and Resilience through Acquisition – Final Report of the Department of Defense and General Services Administration

Section 8(e) of Executive Order (EO) 13636 directed that we make recommendations to you on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration.

Attached is the final signed report of the Department of Defense and General Services Administration Joint Working Group on Improving Cybersecurity and Resilience through Acquisition, one component of the Government-wide implementation of EO 13636 and Presidential Policy Directive 21.

Chuck Hagel
Secretary of Defense

Daniel M. Tangherlini
Administrator of General Services

Attachment:
As stated

Improving Cybersecurity and Resilience through Acquisition

Final Report of the Department of Defense and General Services Administration

November 2013

The estimated cost of this report or study for the Department of Defense is approximately $208,000 in FY 2012-2013.
Cost estimate generated on November 13, 2013 RefID: 5-C493D22

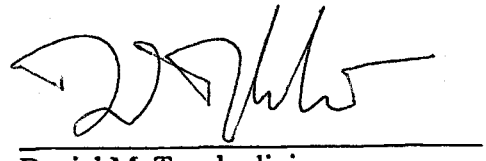
This Page Intentionally Left Blank

Foreword

The Department of Defense and the General Services Administration have prepared this report to the President in accordance with Executive Order 13636. The report provides a path forward to aligning Federal cybersecurity risk management and acquisition processes.

The report provides strategic guidelines for addressing relevant issues, suggesting how challenges might be resolved, and identifying important considerations for the implementation of the recommendations. The ultimate goal of the recommendations is strengthening the cyber resilience of the Federal government by improving management of the people, processes, and technology affected by the Federal Acquisition System.

Frank Kendall
Under Secretary of Defense
Acquisition, Technology, and Logistics



Daniel M. Tangherlini
Administrator of General Services

Preface

This document constitutes the final report of the *Department of Defense (DoD) and General Services Administration (GSA) Joint Working Group on Improving Cybersecurity and Resilience through Acquisition.* The report is one component of the government-wide implementation of Executive Order (EO) 13636 and Presidential Policy Directive (PPD) 21. It was developed in collaboration with stakeholders from Federal agencies and industry and with the assistance of the Department of Homeland Security's Integrated Task Force.[1] The Working Group also coordinated development of the recommendations closely with the Department of Commerce, National Institute of Standards and Technology's (NIST) development of a framework to reduce cyber risks to critical infrastructure[2] (Cybersecurity Framework), and in parallel to the Departments of Commerce, Treasury, and Homeland Security reports on incentives to promote voluntary adoption of the Cybersecurity Framework.[3] This jointly issued report is the culmination of a four-month process by an interagency working group comprised of topic-knowledgeable individuals selected from the Federal government.[4]

One of the major impediments to changing how cybersecurity is addressed in Federal acquisitions is the differing priorities of cyber risk management and the Federal Acquisition System.[5] The Acquisition Workforce[6] is required to fulfill numerous, sometimes conflicting, policy goals through their work, and cybersecurity is but one of several competing priorities in any given acquisition. The importance of cybersecurity to national and economic security dictates the need for a clear prioritization of cyber risk management as both an element of enterprise risk management and as a technical requirement in acquisitions that present cyber risks. The importance of cybersecurity relative to the other priorities in Federal acquisition should be made explicit.

The purpose of this report is to recommend how cyber risk management and acquisition processes in the Federal government can be better aligned. The report does not provide explicit implementation guidance, but provides strategic guidelines for addressing relevant issues, suggesting how challenges might be resolved and identifying important considerations for the implementation of the recommendations.

---

[1] The Department established an Integrated Task Force (ITF) to lead DHS implementation and coordinate interagency, and public and private sector efforts; see, http://www.dhs.gov/publication/integrated-task-force.
[2] 78 Fed. Reg. 13024 (February 26, 2013).
[3] *See*, 78 Fed. Reg. 18954 (March 28, 2013).
[4] Appendix I contains a list of the Working Group members.
[5] See, 48 C.F.R. § 1.102 (2013).
[6] *Id.*

TABLE OF CONTENTS

Executive Summary

When the government purchases products or services with inadequate in-built cybersecurity, the risks persist throughout the lifespan of the item purchased. The lasting effect of inadequate cybersecurity in acquired items is part of what makes acquisition reform so important to achieving cybersecurity and resiliency. Purchasing products and services that have appropriate cybersecurity designed and built in may have a higher up-front cost in some cases, but doing so reduces total cost of ownership by providing risk mitigation and reducing the need to fix vulnerabilities in fielded solutions.

Increasingly, the Federal government relies on network connectivity, processing power, data storage, and other information and communications technology (ICT) functions to accomplish its missions. The networks the government relies on are often acquired and sustained through purchases of commercial ICT products and services. These capabilities greatly benefit the government, but have also, in some cases, made the government more vulnerable to cyber attacks and exploitation.

Resilience to cyber risks has become a topic of core strategic concern for business and government leaders worldwide and is an essential component of an enterprise risk management strategy. While the report focuses its recommendations on increasing the use of cybersecurity standards in Federal acquisitions,[7] DoD and GSA view the ultimate goal of the recommendations as strengthening the cyber resilience of the Federal government by improving management of the people, processes, and technology affected by the Federal Acquisition System.

It is important to note that these recommendations are not intended to conflict with acquisition or cybersecurity requirements related to National Security Systems (NSS). The Committee on National Security Systems (CNSS) is responsible for the creation and maintenance of National-level Information Assurance operating issuances for NSS and for providing a comprehensive forum for strategic planning and operational decision-making to protect NSS for the United States.[8] The CNSS has also established acquisition practices for NSS, and those practices are explicitly not within the scope of this report.[9] The

---

[7] The terms "Federal acquisition(s)," or "acquisition(s)," are used throughout this report to mean all activities of Departments and Agencies to acquire new or modified goods or services, including strategic planning, capabilities needs assessment, systems acquisition, and program and budget development. See, e.g., "*Big "A" Concept and Map*," available at, https://dap.dau.mil/aphome/Pages/Default.aspx.

[8] The Committee on National Security Systems (CNSS) has been in existence since 1953. The CNSS (formerly named the National Security Telecommunications and Information Systems Security Committee (NSTISSC)) was established by National Security Directive (NSD)-42, "National Policy for the Security of National Security Telecommunications and Information Systems. This was reaffirmed by Executive Order (E.O.) 13284, dated January 23, 2003, "Executive Order Amendment of Executive Orders and Other Actions in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security" and E.O. 13231, "Critical Infrastructure Protection in the Information Age" dated October 16, 2001. Under E.O. 13231, the President re-designated the NSTISSC as CNSS. The Department of Defense continues to chair the Committee under the authorities established by NSD-42.

[9] OMB policies (including OMB Reporting Instructions for FISMA and Agency Privacy Management) state that for other than national security programs and systems, federal agencies must follow certain specific NIST Special Publications. See, e.g., *Guide for Applying the Risk Management Framework to Federal Information System:*

recommendations are intended to complement and align with current processes and practices used to acquire NSS and were developed in consultation with organizations that routinely acquire NSS, including the Defense Intelligence Agency, National Security Agency, the Federal Bureau of Investigation, and the Department of Justice Office of the Chief Information Officer.

These recommendations were not created in isolation. Rather, the recommendations are designed to be considered as one part of the Federal Government's comprehensive response to cyber risks. Furthermore, the recommendations do not explicitly address how to harmonize rules. Instead, the recommendations focus on driving consistency in interpretation and application of procurement rules and incorporation of cybersecurity into the technical requirements of acquisitions. The recommendations are summarized as follows:

I. ***Institute Baseline Cybersecurity Requirements as a Condition of Contract Award for Appropriate Acquisitions.***
Basic cybersecurity hygiene is broadly accepted across the government and the private sector as a way to reduce a significant percentage of cyber risks. For acquisitions that present cyber risks, the government should only do business with organizations that meet such baseline requirements in both their own operations and in the products and services they deliver. The baseline should be expressed in the technical requirements for the acquisition and should include performance measures to ensure the baseline is maintained and risks are identified.

II. ***Address Cybersecurity in Relevant Training.***
As with any change to practice or policy, there is a concurrent need to train the relevant workforces to adapt to the changes. Incorporate acquisition cybersecurity into required training curricula for appropriate workforces. Require organizations that do business with the government to receive training about the acquisition cybersecurity requirements of the organization's government contracts.

III. ***Develop Common Cybersecurity Definitions for Federal Acquisitions.***
Unclear and inconsistently defined terms lead, at best, to suboptimal outcomes for both efficiency and cybersecurity. Increasing the clarity of key cybersecurity terms in Federal acquisitions will increase efficiency and effectiveness for both the government and the private sector. Key terms should be defined in the Federal Acquisition Regulation.

IV. ***Institute a Federal Acquisition Cyber Risk Management Strategy.***
From a government-wide cybersecurity perspective, identify a hierarchy of cyber risk criticality for acquisitions. To maximize consistency in application of procurement rules, develop and use "overlays"[10] for similar types of acquisition, starting with the types of

---

A Security Life Cycle Approach, NIST Special Publication 800-37, Revision 1 (Feb. 2010), and *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, Revision 4, (Apr. 2013).

[10] An overlay is a fully specified set of security requirements and supplemental guidance that provide the ability to appropriately tailor security requirements for specific technologies or product groups, circumstances and conditions, and/or operational environments.

acquisitions that present the greatest cyber risk.

V. ***Include a Requirement to Purchase from Original Equipment Manufacturers, Their Authorized Resellers, or Other "Trusted" Sources, Whenever Available, in Appropriate Acquisitions.***
In certain circumstances, the risk of receiving inauthentic or otherwise nonconforming items is best mitigated by obtaining required items only from original equipment manufactuers, their authorized resellers, or other trusted sources. The cyber risk threshold for application of this limitation of sources should be consistent across the Federal government.

VI. ***Increase Government Accountability for Cyber Risk Management.***
Identify and modify government acquisition practices that contribute to cyber risk. Integrate security standards into acquisition planning and contract administration. Incorporate cyber risk into enterprise risk management and ensure key decision makers are accountable for managing risks of cybersecurity shortfalls in a fielded solution.

Implementation of the recommendations should be precisely aligned with the extensive ongoing critical infrastructure and cybersecurity efforts of industry and government, most importantly the Comprehensive National Cybersecurity Initiative and the Cybersecurity Framework being developed under the Executive Order, but also the National Infrastructure Protection Plan (NIPP), the associated Sector Specific Plans, information sharing efforts on threat and vulnerability issues, the sectors' various risk assessment and risk management activities, and statutory and regulatory changes.

Cybersecurity standards are continually being established and updated through the transparent, consensus-based processes of standards development organizations (SDO).[11] Many of these processes are international in design and scope, and they routinely include active engagement by multinational corporations and various government entities that participate as developers or users of the technology. Organizations voluntarily adopt the resulting best practices and standards to best fit their unique requirements, based on their roles, business plans, and cultural or regulatory environments. The international standards regime facilitates interoperability between systems and a competitive commercial market. It also spurs the development and use of innovative and secure technologies.

Incorporation of voluntary international standards and best practices into Federal acquisitions can also be highly effective in improving cybersecurity and resilience. However, Federal agencies are required to use standards and guidelines that are developed and implemented through NIST.[12] Cybersecurity standards used in acquisitions should align to the greatest extent possible with international standards and emphasize the importance of organizational flexibility in application. Flexibility is critical to addressing dynamic threats and

[11] This includes, but is not limited to, established SDOs like ISO/IEC JTC1 and related standards (27001/2, 15408, etc.) as well as work from other international SDOs.
[12] 40 USC § 11302(d) (2013).

developing workable solutions for the widely disparate configurations and operational environments across the Federal government.

Several related changes to the acquisition rules are also underway and must be addressed prior to implementing these recommendations. Where the recommendations are closely aligned with an ongoing Federal Acquisition Regulation (FAR) or Defense Federal Acquisition Regulation Supplement (DFARS) rulemaking, a specific reference is provided. In general, implementation must be harmonized with, and be built upon as appropriate, existing international and consensus based standards, as well as statutes and regulations applicable to this field, including the Federal Information Security Management Act of 2002 (FISMA),[13] the Clinger Cohen Act of 1996,[14] the Department of Homeland Security Appropriations Act of 2007,[15] and related sections of the National Defense Authorization Acts,[16] among numerous others. Finally, implementation must be coordinated with the independent regulatory agencies.

While it is not the primary goal, implementing these recommendations may contribute to increases in cybersecurity across the broader economy, particularly if changes to Federal acquisition practices are adopted consistently across the government and concurrently with other actions to implement the Cybersecurity Framework. However, other market forces – more specifically, broad customer demand for more secure ICT products and services – will have a greater impact on the Nation's cybersecurity baseline than changes in Federal acquisition practices.[17]

Changes to the Federal Acquisition System therefore should be focused on strengthening the cybersecurity knowledge, practices, and capabilities within the Federal government's network and domain. The implementation approach should leverage the existing system of voluntary international standards development and the Cybersecurity Framework. The government should start by changing its own practices that increase cyber risk and focus on the types of acquisitions that present the greatest cyber risk and in which investment of scarce resources will provide the greatest return overall.

Background

On February 12, 2013, the President issued Executive Order 13636[18] for Improving Critical Infrastructure Cybersecurity (EO) directing Federal agencies to use their existing

---

[13] 44 U.S.C. § 3541 et seq.
[14] 40 U.S.C. §11101 et seq.
[15] P.L. 109-295, 120 Stat. 552.
[16] See, e.g., Section 806, Ike Skelton National Defense Authorization Act for Fiscal Year 2011, Pub. L. 111-383 (Jan. 7, 2011).
[17] Input received in response to the Working Group's published Request for Information asserts that the Federal government's buying power in the global ICT marketplace, while significant, is insufficient to create a universal change in commercial practices, and reliance on this procurement power alone to shift the market will result in a number of suppliers choosing not to sell to the Federal government. See, General Services Administration (GSA) Notice: Joint Working Group on Improving Cybersecurity and Resilience through Acquisition; Notice-OERR-2013-01, available at http://www.regulations.gov/#!documentDetail;D=GSA-GSA-2013-0002-0030.
[18] Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

authorities and increase cooperation with the private sector to provide stronger protections for public and private sector cyber-based systems that are critical to our national and economic security. In accordance with the EO, GSA and DoD established the Working Group to fulfill the requirements of Section 8(e) of the Executive Order, specifically:

> *"(e) Within 120 days of the date of this order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary and the Federal Acquisition Regulatory Council, shall make recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. The report shall address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity."*[19]

By highlighting the need to address feasibility, security benefits, and relative merits of increasing the use of security standards in Federal acquisitions, the EO highlights the need to effectively balance responses to cyber risks against the increased costs those responses might create. Furthermore, consistency in application of procurement rules can drive additional efficiencies.

Cyber Risk and Federal Acquisition

Federal acquisition is a cross-cutting function that directly impacts operations in all departments and agencies. It is most importantly a means to an end – delivery of something that will enable government to accomplish its missions. An end user is most concerned that the output of the process is delivery of the capability that meets the need. However, the acquisition of a capability is only part of the lifecycle, or series of lifecycles, where cyber risks are present.

Increasingly, the Federal government relies on network connectivity, processing power, data storage, and other information and communications technology (ICT) functions, to accomplish its missions. The networks the government relies on are often acquired and sustained through purchases of commercial ICT products and services. These increased capabilities have greatly benefitted our government, but have also, in some cases, made the government more vulnerable to cyber attacks and exploitation.

The Federal government spends more than $500 billion a year for a range of goods and services required to meet mission needs. This amount of spending is large, but in the global context,[20] it represents less than 1 percent of the total market. So while the Federal government is a significant customer, its ability to effect broad market changes through its purchasing is less significant.

---

[19] *Id.*

[20] https://www.cia.gov/library/publications/the-world-factbook/geos/xx.html.

Procurement of commercial items is encouraged in Federal acquisitions, in part by the availability of price competition, but more importantly because it provides immediate access to rapidly evolving technology. Offshore sourcing has demonstrated its merit as a means to reduce costs, and as a result most commercial items are now produced in a global supply chain. Movement of production outside the United States has also led to growing concerns associated with foreign ownership, control, manipulation, or influence over items that are purchased by the government and used in or connected to critical infrastructure or mission essential systems.

Importantly, the problem is not a simple function of geography. Pedigree[21] is a sub-set of factors to consider in cyber risk assessments, yet there are more important factors in addressing the security or integrity of components and end items, including careful attention to the people, processes, and technology used to develop, deliver, operate, and dispose of the products and services used by the government and its contractors.

The modern ICT supply chain is a complex, globally distributed system of interconnected value-networks that are logically long with geographically diverse routes and multiple tiers of international sourcing. This system of networks includes organizations, people, processes, products, and services, and extends across the full system development life cycle, including research and development, design, development, acquisition of custom or commercial products, delivery, integration, operations, and disposal/retirement.

Vulnerabilities can be created intentionally or unintentionally and can come from inside or outside of the supply chain itself. The cyber threat presented by U.S. adversaries (foreign governments, militaries, intelligence services, and terrorist organizations) and those seeking to advance their own cause (hackers and criminal elements) without regard to U.S. national security interests, law enforcement activities, or intellectual property rights has introduced significant new risk to the Federal government and industry. The Federal government and its contractors, subcontractors, and suppliers at all tiers of the supply chain are under constant attack, targeted by increasingly sophisticated and well-funded adversaries seeking to steal, compromise, alter or destroy sensitive information. In some cases, advanced threat actors target businesses deep in the government's supply chain to gain a foothold and then "swim upstream" to gain access to sensitive information and intellectual property. However, it is important to note that most known intrusions are not caused by an adversary intentionally inserting malicious code into an ICT component through its supply chain, but are made through exploitation of unintentional vulnerabilities in code or components (e.g. remote access attacks). Nevertheless, both intentional and unintentional vulnerabilities increase risks. To achieve cyber resiliency, the Federal government must ensure it is capable of mitigating the risks of emerging threats.

The majority of Federal technical information resides on information systems susceptible to the threats and vulnerabilities described above. Therefore, the government must also take into account the risk of this information being targeted for cyber espionage campaigns. This

[21] Pedigree is concerned with the original creation and subsequent treatment of ICT hardware or software, including computational objects such as programs and data, and changes from one medium to another. It emphasizes integrity, chain of custody and aggregation rather than content. It is a tool for establishing trust and accountability in information or an end item. See, e.g., Wohlleben, Paul, *Information Pedigree*, (July 29, 2010); available at: http://www.fedtechmagazine.com/article/2010/07/information-pedigree.

information is often unclassified, but it includes data and intellectual property concerning mission-critical systems requirements, concepts of operations, technologies, designs, engineering, systems production, and component manufacturing. Compromises of this information would seriously impact the operational capabilities of Federal systems.

Recently, the problem of counterfeit, "grey market," or other nonconforming ICT components and subcomponents has gained significant attention as well. These materials can be introduced into systems during both initial acquisition and sustainment. As they are unlikely to have the benefit of testing and maintenance appropriate to their use, they create vulnerabilities for the end customer and increase the likelihood of premature system failure or create latent security gaps that would enable an adversary.

Additionally, significant risks are also presented in the operations and maintenance phase and the disposal process. For example, failure to maintain up to date security profiles, install a software patch in a timely fashion, or failing to include identity and access management requirements all introduce cyber risks, but can be managed through the ICT acquisition process. Similarly, an adversary could extract valuable data from improperly destroyed media. An industry stakeholder submitted that the risk of a commercial entity being sued because of improper data disposal is three times greater than the risk of legal action stemming from a data breach caused by loss or theft and six times greater than from data breaches involving the loss of financial information.[22] In addition, the ICT supply chain is vulnerable to events such as intellectual property theft,[23] service availability disruption,[24] and the insertion of counterfeits.[25] When dealing with a critical system or component, the consequences of these events can be significant, impacting the safety, security, and privacy of potentially millions of people.

While the commercial ICT supply chain is not the source of all cyber risk, it presents opportunity for creation of threats and vulnerabilities, and commercial ICT enables the connectivity that is a necessary element for cyber exploitation. Furthermore, when the Federal government acquires a solution that has inadequate cybersecurity "baked in," the government incurs increased risk throughout the lifespan and disposal of the product or service, or at least until it incurs the added cost of "bolting on" a fix to the vulnerability. It is the lasting effects of inadequate cybersecurity in fielded solutions that makes acquisition so important to achieving cybersecurity and resiliency. Purchasing products and services that have cybersecurity designed and built in may be more expensive in some cases, but doing so reduces total cost of ownership by providing risk mitigation and reducing the need to fix vulnerabilities during use and disposal.

An important way to mitigate cyber risk is adherence to security standards. Federal contracts currently require conformance to a variety of security standards as published in the

---

[22] Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition, Request for Information, 78 Fed. Reg. 27966 (May 13, 2013) (hereinafter, "GSA RFI").

[23] See, e.g., "*IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property,*" 2, The National Bureau of Asian Research (May 2013).

[24] See, e.g., "*White Paper: Managing Cyber Supply Chain Risks,*" 5, Advisen Inc., (May 2013); available at: http://www.onebeaconpro.com/sites/OneBeaconPro/blind/Advisen%20Supply%20Chain%20Risks%20Report.pdf.

[25] See, e.g., Section 818 "Detection and Avoidance of Counterfeit Electronic Parts," FY 2012 NDAA (PL 112 -81); and Defense Federal Acquisition Regulation Supplement: Detection and Avoidance of Counterfeit Electronic Parts (DFARS Case 2012-D055), Proposed Rule, 78 Fed. Reg. 28780 (May 16, 2013).

Federal Acquisition Regulation, Defense Federal Acquisition Regulation Supplement, General Services Administration Acquisition Manual, and Homeland Security Acquisition Manual. The government can immediately increase the value it obtains through the use of security standards in a cost-effective way by increasing the degree of specificity and consistency with which it applies standards to requirements in its contracts.[26] This can be accomplished by ensuring contractual requirements are explicit as to which standards, and more specifically, which sections of particular standards, need to be applied against explicitly articulated security needs for the acquired item.

A selective approach to this task is appropriate because all acquisitions do not present the same level of risk. For some acquisitions, basic cybersecurity measures are all that is required to adequately address the risks, and for other acquisitions, additional cybersecurity controls are required. The differences are primarily driven by the variations in fitness for use of the acquired items, which is closely related to the risk tolerance of the end user. For example, the same printer/copier procured to perform the same function by two different organizations might legitimately require different security protections based on operational environments and end users. Differences in risk tolerance between end users can be based on, among numerous other things, differences in information sensitivity and mission criticality that are associated with specific department and agency technical implementations.

The government must work to ensure that there is not a mismatch between mission-based cybersecurity requirements for product assurance or connectivity and what it is actually purchasing. It is important to note that implementation must be consistent with U.S. obligations under international agreements, and voluntary international standards should be applied whenever possible in Federal acquisitions. Ultimately, the government must continue striving to make innovation the standard in improving cybersecurity.

Recommendations

Commercial ICT is ubiquitous in Federal networks, even those that handle the most sensitive information and support essential functions of the government. Therefore, the recommendations focus primarily on exposure to cyber risks related to acquisitions of ICT and how those risks should be addressed. However, due to the increasing connectivity of the world and the growing sophistication of threats, the recommendations apply equally to acquisitions that are outside the boundaries of traditional definitions of ICT.

I. Institute Baseline Cybersecurity Requirements as a Condition of Contract Award for Appropriate Acquisitions.

Baseline cybersecurity refers to first-level information and security measures used to deter unauthorized disclosure, loss, or compromise. Basic protections such as[27] updated virus

[26] In some circumstances, this will reduce costs by reducing the level of effort required by the contractor to figure out which specific controls in a standard apply to the acquisition; see e.g., Microsoft response to GSA RFI, available at http://www.regulations.gov/#!documentDetail;D=GSA-GSA-2013-0002-0005.

[27] This list is intended to be illustrative only.

protection, multiple-factor logical access, methods to ensure the confidentiality of data, and current security software patches are broadly accepted across government and the private sector as ways to reduce a significant percentage of cyber risks. When the Federal government does business, directly or indirectly, with companies that have not incorporated baseline cybersecurity protections into their own operations and products, the result is increased risk. Ensuring that the people, processes, and technology with access to assets at risk are employing baseline requirements raises the level of cybersecurity across the Federal enterprise.

First-level protective measures are typically employed as part of the routine course of doing business. The cost of not using basic cybersecurity measures would be a significant detriment to contractor and Federal business operations, resulting in reduced system performance and the potential loss of valuable information. It is also recognized that prudent business practices designed to protect an information system are typically a common part of everyday operations. As a result, the benefit of protecting and reducing vulnerabilities to information systems through baseline cybersecurity requirements offers substantial value to contractors and the Government.

The baseline should be expressed in the technical requirements for the acquisition and should include performance measures to ensure the baseline is maintained and risks are indentified throughout the lifespan of the product or service acquired. Due to resource constraints and the varying risk profiles of Federal acquisitions, the government should take an incremental, risk-based approach to increasing cybersecurity requirements in its contracts beyond the baseline.

As a preliminary matter, cybersecurity requirements need to be clearly and specifically articulated within the requirements of the contract. Often, cybersecurity requirements are expressed in terms of compliance with broadly stated standards and are included in a section of the contract that is not part of the technical description of the product or service the government seeks to acquire.[28] This practice leaves too much ambiguity as to which cybersecurity measures are actually required in the delivered item. This recommendation envisions requirements for baseline cybersecurity requirements for contractor operations as well as products or services delivered to the government.

This recommendation is intended to be harmonized with the ongoing FAR and DFARS rulemakings entitled "Basic Safeguarding of Contractor Information Systems,"[29] and "Safeguarding Unclassified Controlled Technical Information."[30]

II. Address Cybersecurity in Relevant Training.

As with any change to practice or policy, there is a concurrent need to train the relevant workforces to adapt to the changes. This is particularly the case when the changes involve major

---

[28] See, Comment on FR Doc # 2013-11239, GSA-GSA-2013-0002-0005, Nicholas, J. Paul, Microsoft Corporation (Jun. 12, 2013), available at http://www.regulations.gov/#!docketBrowser;rpp=100;so=DESC;sb=docId;po=0;dct=PS;D=GSA-GSA-2013-0002.

[29] 77 Fed. Reg. 51496 (Aug. 24, 2012), Proposed rule, FAR Case 2011-020.

[30] DFARS Case 2011-D039, Interim Rule, under review by Office of Information and Regulatory Affairs (last accessed, June 10, 2013, http://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf).

shifts in behavior, like the risk management changes outlined in these recommendations. Additionally, the government should implement an acquisition cybersecurity outreach campaign targeted at industry stakeholders.[31] The training overall, and the industry engagement in particular, should clearly articulate that the government is changing its buying behavior relative to cybersecurity by adopting a risk-based methodology, and as a result, the government will require more from industry relative to cybersecurity in certain types of acquisition.

Increasing the knowledge of the people responsible for doing the work will facilitate appropriate cyber risk management and help avoid over-specifying cybersecurity requirements (which leads to higher costs) or under-specifying cybersecurity requirements (which leads to greater risks).

III. Develop Common Cybersecurity Definitions for Federal Acquisitions.

Increasing the clarity of key cybersecurity terms in Federal acquisitions will increase the efficiency and effectiveness of both the government and the private sector. The ability to effectively develop and fulfill requirements depends in large part on a shared understanding of the meaning each party assigns to a key terms, especially in specialized professional disciplines like cybersecurity and acquisition. This need is especially acute when these terms are included in legal instruments as part of the acquisition process.

Unclear and inconsistently defined terms lead, at best, to suboptimal outcomes for both efficiency and cybersecurity. When misunderstandings persist in the acquisition process, they may create inaccuracy or confusion about technical requirements, market research, cost estimates, budgets, purchase requests, solicitations, proposals, source selections, and award and performance of contracts. In operational activities governed by legal instruments, varying definitions can be much more difficult to address and create very real cost impacts, including contractual changes, terminations, and litigation. A good baseline for these definitions is found in consensus based, international standards.

This recommendation is intended to be harmonized with the ongoing DFARS rulemaking entitled "Detection and Avoidance of Counterfeit Electronic Parts."[32]

IV. Institute a Federal Acquisition Cyber Risk Management Strategy.

The government needs an interagency acquisition cyber risk management strategy that requires agencies to ensure their performance meets strategic cyber risk goals for acquisition and is part of the government's enterprise risk management strategy. The strategy should be based on a government-wide perspective of acquisition and be primarily aligned with the methodologies and procedures developed to address cyber risk in the Cybersecurity Framework.

---

[31] E.g., GSA provides training about its Multiple Award Schedules (MAS) program through the "Pathway to Success" training. This is a mandatory training module that provides an overview of GSA MAS contracts. Potential offerors must take the "Pathway To Success" test prior to submitting a proposal for a Schedule contract. See, https://vsc.gsa.gov/RA/research.cfm. Additionally, contractors might, in certain circumstances, be required to complete ongoing training throughout contract performance. Specific training about an acquisition might also be included in requirements to become a qualified bidder, and become a source selection criterion.

[32] 78 Fed. Reg. 28780 (May 16, 2013), Proposed Rule; DFARS Case 2012-D055.

It should identify a hierarchy of cyber risk criticality for acquisitions and include a risk-based prioritization of acquisitions. The risk analysis should be developed in alignment with the Federal Enterprise Architecture[33] and NIST Risk Management Framework (RMF).[34]

The strategy should include development of "overlays:" fully specified sets of security requirements and supplemental guidance that provide the ability to appropriately tailor security requirements for specific technologies or product groups, circumstances and conditions, and/or operational environments.[35]

When developing the strategy, the government should leverage existing risk management processes and data collection methodologies and consistently incorporate cyber risk as an element of enterprise risk management. The strategy should encompass standard network security practices to address vulnerability of information to cyber intrusions and exfiltration. The strategy should leverage supply chain risk management processes to mitigate risks of non-conforming items (such as counterfeit and tainted products). And it should include appropriate metrics to define risk and to measure the ability of agencies to apply empirical risk modeling techniques that work across both public and private organizations. In developing the strategy, the government should use the active, working partnerships between industry, the civilian agencies, and the intelligence community, and create such partnerships where they do not already exist, with the goal of leveraging validated and outcome-based risk management processes, best practices, and lessons learned.

Where appropriately defined categories of similar types of acquisitions already exist,[36] the government should develop overlays for those types of acquisitions. The overlays should be developed in collaboration with industry, and consistently applied to all similar types of Federal acquisitions. The starting point for development of the requirements should be the Cybersecurity Framework.

The overlays should encompass realistic, risk-based controls that appropriately mitigate the risks for the type of acquisition and should define the minimum acceptable controls for any acquisition that is of a similar type. The overlays should not, as a general rule, incorporate standards directly into contracts and should avoid prescriptive mandates for specific practices, tooling, or country-specific standards, because the inflexibility of those approaches often inadvertently increases costs without actually reducing risk.[37] Instead, the overlays should

---

[33] Available at http://www.whitehouse.gov/omb/e-gov/fea/.

[34] See, NIST Special Publication 800-37, Revision 1 (Feb. 2010).

[35] See, e.g., The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Available at: http://www.gsa.gov/portal/category/102375. See also, the Information Systems Security Line of Business (ISSLoB) is a comprehensive and consistently implemented set of risk-based, cost-effective controls and measures that adequately protects information contained in federal government information systems. Available at: http://www.dhs.gov/information-systems-security-line-business.

[36] See, e.g., FedRAMP, ISSLoB, and Federal Strategic Sourcing Initiative (FSSI) (available at: http://www.gsa.gov/fssi.), among others. These programs have defined categories of similar types of products and services.

[37] Directly incorporating standards could freeze the status quo and hamper or prevent the evolution of countermeasures required to address the dynamic threat and technology landscapes. It might also create a risk that other nations will adopt similar mandates which could further increase supply chain costs. Incorporating

specifically identify security controls from within standards that should be applied to the type of acquisition being conducted. The overlays should also include acquisition and contractual controls like source selection criteria and contract performance measures. Finally, to the greatest extent possible, the overlays should be expressed as technical requirements. This approach will allow the government to describe top-level cybersecurity requirements, decompose them to a lower level for an individual acquisition, and then articulate them consistent with and in a similar manner as other requirements for the fielded solution.

This recommendation is based on the fact that not all assets delivered through the acquisition system present the same level of cyber risk or warrant the same level of cybersecurity, and requiring increased cybersecurity in planning and performance of government contracts creates cost increases for contractors and the Federal government. Such cost increases must be balanced against the nature and severity of cyber risks and the corresponding cost or performance reductions in other functionality. The Federal government can mitigate the amount of any cost increases if it creates certainty by adopting cybersecurity requirements across market segments and similar types of procurement.

V. Include a Requirement to Purchase from Original Equipment or Component Manufacturers, Their Authorized Resellers, or Other "Trusted" Sources, Whenever Available, in Appropriate Acquisitions.

Ensuring that the goods provided to the government are authentic and have not been altered or tampered with is an important step in mitigating cyber risk. Inauthentic end items and components often do not have the latest security-related updates or are not built to the original equipment (or component) manufacturer's (OEM) security standards. In certain circumstances, the risk of receiving inauthentic, counterfeit, or otherwise nonconforming items is best mitigated by obtaining required items only from OEMs, their authorized resellers, or other trusted sources.[38]

OEMs have a heightened interest in ensuring the authenticity of their products, and this interest carries through into their policies for designating certain suppliers or resellers as "authorized." Limiting eligibility to only these types of sources for *all* acquisitions may not be compatible with acquisition rules, socioeconomic procurement preferences, or principles of open competition. Additional trusted sources can be identified through the use of qualified products, bidders, or manufacturers lists (QBL)[39] to ensure that identified sources meet appropriate standards for providing authentic items. The QBLs should be based on the cyber risk mitigation value provided by the use of the trusted source.

---

government-specific standards that would duplicate existing security-related standards or creating country-specific requirements that could restrict the use of long-standing and highly credible global suppliers of technology could have significant negative effects on the government's ability to acquire the products and services it needs.

[38] See, e.g., Solutions for Enterprise Wide Procurement (SEWP) V, is a multiple-award Government-Wide Acquisition Contract (GWAC) that provides IT Products and Product Solutions. SEWP is administered by NASA, and the recently released draft RFP includes this limitation of sources by requiring offerors for certain types of items to be an authorized reseller of the OEM; available at https://www.sewp.nasa.gov/sewpv/.

[39] 48 C.F.R. § 9.203 (2013).

Even with use of trusted sources, it may be possible to have "authentic" equipment that still has cyber vulnerabilities. This approach also represents a limitation of available sources and therefore should only be used for types of acquisition that present risks great enough to justify the negative impact on competition or price differences between trusted and un-trusted sources. For acquisitions that present these types of risks, the government should limit sources to OEMs, authorized resellers, and trusted suppliers, and the qualification should be incorporated into the full acquisition and sustainment life cycles, starting with requirements definition, acquisition planning, and market research.

If the government chooses to use a reseller, distributor, wholesaler, or broker that is not in a trusted relationship with the OEM, then the government should obtain assurances of the company's ability to guarantee the security and integrity of the item being purchased. Such a trusted supplier compliance requirement is especially important when acquiring obsolete, refurbished, or otherwise out-of-production components and parts.

The terms and conditions a supplier or reseller must meet to obtain status as a "trusted" source will vary between market segments, but in general suppliers will be assessed against a broad set of criteria including long-term business viability, quality control systems, order placement and fulfillment processes, customer support, customer returns policies, and past record, such as by a search in Government-Industry Data Exchange Program[40] (GIDEP). In order to establish QBLs, the substance and application of these criteria must be evaluated by the government, or a third party authorized by the government, on a regular basis to ensure the QBL designation provides continued value in actually mitigating cyber risk.

The method by which the government conducts the evaluations should be based on the cyber risk of the acquisition type. For example, for acquisition types that present the greatest risk, the appropriate evaluation method might be an audit performed by government personnel. For less risky categories, the appropriate evaluation method might be first, second, or third party attestation of company conformance to a standard. At a minimum, the qualification program should be based on the Cybersecurity Framework, have consistent and well defined processes for validation and testing, consider the use of third parties to conduct reviews and approvals, and include enforcement mechanisms.

VI. Increase Government Accountability for Cyber Risk Management.

As described above, Federal systems are subject to cyber risks throughout the development, acquisition, sustainment, and disposal life cycles. The application of cyber risk management practices must similarly cut across all phases and functionality, including but not limited to, technology and development; engineering and manufacturing; production; operations and support; security; and counterintelligence. The success of such practices will be dependent upon the integration of cybersecurity risks into existing acquisition processes to inform key stakeholders and decision makers from each of these phases and functions.

---

[40] GIDEP is a cooperative activity between government and industry participants seeking to reduce or eliminate expenditures of resources by sharing technical information. Since 1959, over $2.1 billion in prevention of unplanned expenditures has been reported. See, http://www.gidep.org.

This recommendation is intended to integrate security standards into acquisition planning and contract administration and incorporate cyber risk into enterprise risk management to ensure that key decision makers are accountable for decisions regarding the threats, vulnerabilities, likelihood, and consequences of cybersecurity risks in the fielded solution.

First, cyber risk should be addressed when a requirement is being defined and a solution is being analyzed. Based on the cybersecurity overlay requirements for the type of acquisition, the requirement developer and acquisition personnel determine which controls should be included in the requirement, identify which risk decisions are critical for the acquisition, and ensure that the critical decisions are informed by key stakeholders and the cyber risk management plan.

Next, prior to release of the solicitation, acquisition personnel should certify that appropriate cybersecurity requirements are adequately reflected in the solicitation. This includes but is not limited to incorporation into technical requirements, pricing methodology, source selection criteria and evaluation plan, and any post-award contract administration applications.

Third, during the source selection process, acquisition personnel should participate in the proposal evaluation process and ensure that the apparent best value proposal meets the cybersecurity requirements of the solicitation.

Finally, to the extent any conformance testing, reviews of technology refreshes, supply chain risk management measures, or any other post-award contract performance matters are relevant to cybersecurity, the accountable individual (e.g. program executive), with the assistance of acquisition personnel, should be required to certify that the activity was conducted in accordance with prescribed standards.

Conclusion

The recommendations in this report address feasibility, benefits, and merits of incorporating standards into acquisition planning and contracts and harmonizing procurement requirements through an initial focus on the need for baseline cybersecurity requirements, broad workforce training, and consistent cybersecurity terminology. These are suggested to be combined with incorporation of cyber risk management into enterprise risk management, development of more specific and standardized use of security controls for particular types of acquisitions, limiting purchases to certain sources for higher risk acquisitions, and increasing government accountability for cybersecurity throughout the development, acquisition, sustainment, use, and disposal life cycles.

The recommendations are much more about changing the behavior of government program managers and acquisition decision makers than they are about changing the behavior of industry segments or contracting officers. The Government cannot make all of its contracting officers into cybersecurity experts, but it can improve the cybersecurity of its acquisitions by ensuring appropriate accountability for cyber risk management is incorporated into the acquisition process. The bottom line is that the government will only achieve the goal of increasing cybersecurity and resilience through acquisitions by making sure its own practices are

not increasing risks unnecessarily. Using the methods outlined in these recommendations will allow the government to make better choices about which cybersecurity measures should be implemented in a particular acquisition. And the choices will be based on disciplined, empirical cyber risk analysis.

Achieving cyber resilience will require investments in the personnel and resources necessary to manage the risks. Building cyber resiliency also requires interagency coordination and cooperation between the public and private sectors (including between supply chain suppliers and providers). It also requires everyone from front-line employees to those in the most senior leadership positions to have greater awareness of the issue.

In summary, the government should approach this complex matter thoughtfully and collaboratively, taking affirmative steps to minimize the adverse impact on the ICT market by ensuring its own policies and practices are part of the solution.

APPENDIX I - JOINT WORKING GROUP ROSTER

The individuals listed in the table below are the core team that drafted the report and developed the recommendations. But there are many other individuals from both public and private sector organizations who also participated substantially. All brought a high degree of professionalism and knowledge to their work, and represented the equities of their organizations, functional disciplines, and the interests of the Federal government in an exemplary manner.

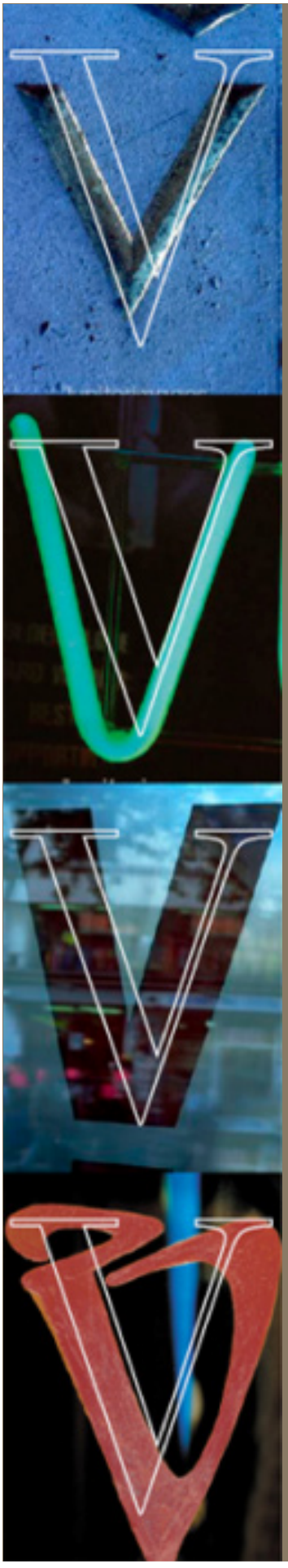
AGENCY	ORGANIZATION	NAME(S)
Department of Defense	Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics; Defense Procurement and Acquisition Policy	Michael Canales Mary Thomas
	Office of the Assistant Secretary of Defense for Cyber Policy	Joshua Alexander
	Office of the Chief Information Officer	Don Davidson Jenine Patterson
General Services Administration	Office of Emergency Response and Recovery	Christopher Coleman
	Federal Acquisition Service	Emile Monette Larry Hale Shondrea Lyublanovits
	Office of Governmentwide Policy	Marissa Petrusek
Office of Management and Budget	Office of Federal Procurement Policy	Jeremy McCrary
Department of Homeland Security	National Protection and Programs Directorate, Office of Cybersecurity and Communications	Joe Jarzombek Michael Echols
	Directorate for Management, Office of the Chief Procurement Officer	Camara Francis Shaundra Duggans
Department of Commerce	National Institute of Standards and Technology	Jon Boyens

APPENDIX II - STAKEHOLDER ENGAGEMENTS

The list below reflects individual engagements with stakeholders conducted by the Working Group as part of the deliberative and report-writing process. This list does not include regular meetings with the DHS ITF, or Working Group meetings. Where the ITF or an agency with members in the Working Group is identified, the engagement was conducted as an adjunct to the regular Working Group and ITF processes, or was a regular engagement that had particular significance (e.g., briefing the draft report to interagency principals).

Date	Engagement
09 Jan 13	TechAmerica
10 Jan 13	Professional Services Council
14 Jan 13	Coalition for Government Procurement
28 Jan 13	TechAmerica
29 Jan 13	Federal Bureau of Investigations
08 Feb 13	TechAmerica
12 Feb 13	Coalition for Government Procurement
15 Feb 13	DHS Integrated Task Force
19 Feb 13	DHS Integrated Task Force
26 Feb 13	Private Company
05 Mar 13	NIST Software Assurance Forum
05 Mar 13	National Defense Industry Associations
08 Mar 13	DHS Integrated Task Force
11 Mar 13	ABA Public Contract Law Section, Cybersecurity Committee
13 Mar 13	NIST Research and Development
14 Mar 13	DHS Incentives Working Group
15 Mar 13	CIPAC IT Sector Coordinating Council, Supply Chain Working Group
21 Mar 13	Private Company
25 Mar 13	CIPAC IT and Communications Sector Coordinating Councils
01 Apr 13	CNCI 11 Working Group
02 Apr 13	Defense Intelligence Agency
02 Apr 13	National Defense Industry Association
04 Apr 13	NIST Designed-in Cybersecurity for Cyber-Physical Systems
04 Apr 13	National Defense Industry Association Cyber Division meeting
16 Apr 13	CIPAC IT Sector Coordinating Council
18 Apr 13	TechAmerica Cybersecurity Committee
19 Apr 13	Professional Services Council
22 Apr 13	CIPAC IT and Communications Sector Coordinating Councils
30 Apr 13	ABA Public Contract Law Section, Cybersecurity Committee meeting
01 May 13	CIPAC IT and Communications Sector Coordinating Councils meeting
01 May 13	Private Company
02 May 13	Semiconductor Industry Association meeting
02 May 13	DHS Integrated Task Force briefing to members
02 May 13	Department of Treasury
03 May 13	Private Company
06 May 13	Private Companies (2)
07 May 13	ACT-IAC Cybersecurity Shared Interest Group meeting

07 May 13	Presentation to interagency at Cyber IPC meeting
09 May 13	Coalition for Government Procurement meeting
13 May 13	Private Companies (2)
14 May 13	Private Company
22 May 13	Internet Security Alliance Board of Directors meeting
22 May 13	National Security Agency, Contracting Policy
22 May 13	Interview, Washington Post
22 May 13	Provided background, Wall Street Journal
23 May 13	Live radio interview, Federal News Radio, "In Depth"
03 Jun 13	Private Companies (5)
03 Jun 13	Department of Treasury
03 Jun 13	Security Industry Association, Government Summit
04 Jun 13	Information Technology Industry Council
04 Jun 13	University of Maryland



Hot Topics in Government Contracts

3:10 p.m. – 4:00 p.m.

Robert A. Burton, Venable LLP

Richard A. Beutel, Committee on Oversight and Government Reform

Paul A. Debolt, Venable LLP

Daniel I. Gordon, George Washington University Law School

VENABLE® LLP

VENABLE® LLP

Venable Government Contracts Symposium
Hot Topics

APRIL 10, 2014

VENABLE® LLP

Panelist Biographies

Robert A. Burton, Venable LLP - Moderator

A thirty-year veteran of procurement law and policy development, Mr. Burton served in the Executive Office of the President as Deputy Administrator of the Office of Federal Procurement Policy (OFPP), the nation's top career federal procurement official. He also served as Acting Administrator for two years during his seven-year tenure at OFPP.

As Deputy Administrator of OFPP, Mr. Burton was responsible for the government's acquisition policy and procurement guidance for all Executive Branch agencies.

His office was charged with developing policy affecting more than $400 billion in annual federal spending – a figure that doubled during Mr. Burton's time in office as a result of the Iraq War and other major events.

At OFPP, Mr. Burton was instrumental on a number of fronts, including preparing the Administration's policy positions and testimony on proposed acquisition legislation; working with House and Senate committees on the development of acquisition reform proposals; and serving as a principal spokesperson for government-wide acquisition initiatives. He also served as the Executive Director of the Chief Acquisition Officers (CAO) Council, which comprises the Chief Acquisition Officers from each federal agency. Mr. Burton also managed the activities of the Federal Acquisition Regulatory (FAR) Council, which has statutory authority to promulgate the government's procurement regulations.

Prior to joining OFPP in 2001, Mr. Burton spent over twenty years as a senior acquisition attorney with the Department of Defense. At the Defense Contract Management Agency, he negotiated the resolution of high-profile contract disputes with major defense contractors and provided advice on cost allowability issues. He served as general counsel for DoD's Defense Energy Support Center, as well as associate general counsel for the Defense Logistics Agency (DLA), the DoD component responsible for purchasing most of the general supplies and services used by the military services. At DLA, Mr. Burton served as counsel to the agency's suspension and debarment official and managed the agency's fraud remedies program, working with the Department of Justice and the criminal investigative agencies to coordinate appropriate remedies in major procurement fraud cases.

Panelist Biographies

Richard A. Beutel, Committee on Oversight and Government Reform

Richard Beutel is currently the Senior Counsel for acquisition and procurement policy for the Committee on Oversight and Government Reform. In that capacity, he is the lead subject matter expert for acquisition and procurement issues on a government-wide basis for Chairman Issa.

For the last 18 months, Rich has served as the legislative manager for the Federal IT Acquisition Reform Act (FITARA), a major overhaul of the governing Clinger Cohen framework. FITARA has cleared OGR Committee mark up and was introduced as part of the latest National Defense Authorization Act. The bill will now go forward as a standalone measure to the floor the week of February 24.

As lead acquisition policy staffer, Rich was also instrumental in moving significant reforms to update the penalties for human trafficking by overseas government contractors and is an expert on expeditionary and contingency contracting practices.

Prior to his service to Chairman Issa, Rich was the General Counsel to the bipartisan Commission on Wartime Contracting in Afghanistan and Iraq. The Wartime Commission was a Congressionally-appointed oversight board mandated by Congress to investigate waste, fraud and abuse in government contracting practices in contingency and wartime operations. As General Counsel, Rich assisted in establishing oversight teams in Afghanistan and Iraq, which identified over $6 billion in wasteful and fraudulent spending. Many of these cases were referred to the Justice Department on a criminal referral.

Prior to his service on the Wartime Commission, Rich reported to Senator Susan Collins, ranking member of the Senate Homeland Security and Government AFFAIRS Committee. In that capacity, Rich was the legislative manager for the Clean Contracting Act provisions in the 2008 National Defense Authorization Act. These provisions significantly reformed the procedures by which Government-wide Acquisition Contracts function. He also served as lead policy staffer on government contract acquisition and policy practices.

Rich's prior government service includes management and policy leadership for the House of Representatives international China program, involving the organization and policy leadership for 12 Congressional and staff delegations to meet with members of the Chinese National People's Congress. He was also a senior executive for Dell, Inc., working directly with Michael Dell for many years in support of Dell's Washington policy initiatives.

Panelist Biographies

Daniel I. Gordon, George Washington University Law School

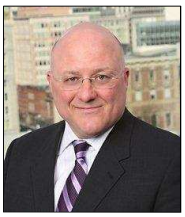
Daniel I. Gordon was appointed Associate Dean for Government Procurement Law at the George Washington University Law School, effective January 1, 2012. Prior to his appointment, he served as the Administrator for Federal Procurement Policy, a position to which he was nominated by President Obama and confirmed by the Senate in 2009. As the Administrator, Mr. Gordon was responsible for developing and implementing acquisition policies supporting over $500 billion in spending by the United States government each year. Prior to joining the Administration, he spent 17 years at the Government Accountability Office (GAO), where he was appointed Deputy General Counsel in 2006 and Acting General Counsel in April 2009.

Before he began at GAO, Mr. Gordon worked in private practice handling acquisition-related matters. Mr. Gordon holds a B.A. from Brandeis University, an M.Phil. from Oxford University, and a J.D. from Harvard Law School. He has also studied in Paris, France; Marburg, Germany; and Tel Aviv, Israel.

Before joining the Administration, Mr. Gordon served as a member of the adjunct faculty at the George Washington University Law School, and he is the author of articles on various aspects of procurement law.

Panelist Biographies

Paul A. Debolt, Venable LLP



Paul Debolt assists companies and individuals on issues that arise from conducting business with the federal government, including civil fraud. He is experienced in the competitive source selection process, defending or prosecuting bid protests, issuing advice concerning compliance with government regulations and laws during the performance of a contract, and helping to resolve disputes and claims during contract performance or as a result of contract termination. Mr. Debolt also counsels clients on the Service Contract Act, the civil False Claims Act, joint ventures and teaming agreements, prime-subcontractor disputes, internal investigations, mandatory disclosures and data rights issues.

Mr. Debolt has extensive government contracts law experience and applies a team approach that ensures clients receive the benefit of firm-wide strength in all related areas.

Discussion

VENABLE LLP

Contact Information

YOUR VENABLE TEAM

Robert A. Burton
rburton@Venable.com
t 202.344.4776
f 202.344.8300

Paul A. Debolt
padebolt@Venable.com
t 202.344.8384
f 202.344.8300

www.Venable.com