

**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.

**SUMMARY:** DoD is issuing a final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to remove coverage on contractors performing private security functions that is now covered in the FAR.

**DATES:** Effective November 18, 2013.

**FOR FURTHER INFORMATION CONTACT:** Ms. Meredith Murphy, telephone 571–372–6098.

**SUPPLEMENTARY INFORMATION:**

**I. Background**

DoD implemented section 862 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2008 (Pub. L. 110–181), as amended by section 853 of the NDAA for FY 2009 (Pub. L. 110–417) and sections 831 and 832 of the NDAA for FY 2011 (Pub. L. 111–383), at DFARS section 225.370 and the clause at 252.225–7039, both entitled “Contractors Performing Private Security Functions.” The DFARS interim rule was published at 76 FR 52133, effective August 19, 2011, and the final rule was published at 77 FR 35883 on June 15, 2012.

These same statutory provisions were subsequently implemented in the FAR at 25.302 and 52.225–26, both entitled “Contractors Performing Private Security Functions Outside the United States,” in FAC 2005–067, issued June 21, 2013. The FAR changes regarding private security contractors were effective on July 22, 2013 (see 78 FR 37670). Therefore, there is no need to retain the duplicative DFARS coverage applicable solely to DoD.

This final rule removes DFARS 225.370 and the clause at 252.225–7039, effective upon publication. In all applicable cases (see FAR 25.302–3, Applicability), the FAR shall be used.

**II. Publication of This Final Rule for Public Comment Is Not Required by Statute**

“Publication of proposed regulations”, 41 U.S.C. 1707, is the statute which applies to the publication of the Federal Acquisition Regulation. Paragraph (a)(1) of the statute requires that a procurement policy, regulation,

procedure or form (including an amendment or modification thereof) must be published for public comment if it relates to the expenditure of appropriated funds, and has either a significant effect beyond the internal operating procedures of the agency issuing the policy, regulation, procedure or form, or has a significant cost or administrative impact on contractors or offerors. This final rule is not required to be published for public comment because DFARS 225.370 and the clause at 252.225–7039 are duplicative of the FAR. Using the FAR clause instead of the DFARS clause should, in effect, be transparent to contractors because the requirements are the same for both clauses.

**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 not a significant regulatory action and, therefore, was not 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**

The Regulatory Flexibility Act does not apply to this rule because this final rule does not constitute a significant DFARS revision within the meaning of FAR 1.501–1 and 41 U.S.C. 1707 does not require publication for public comment.

**V. Paperwork Reduction Act**

This rule affects the information collection requirements in the provisions at DFARS 225.370 and 252.225–7039, currently approved under OMB Control Number 0704–0460,

titled Synchronized Predeployment and Operational Tracker (SPOT) System, in accordance with the Paperwork Reduction Act (44 U.S.C. chapter 35). The information collection requirements associated with OMB 0704–0460 are broader than those applicable only to private security contractors, and the majority of the 0704–0460 requirements (i.e., those not associated with private security contractors) will continue to apply to DoD contractors under the clause at DFARS 252.225–7040. The information collection requirements associated with contractor employees performing private security functions will continue to apply to DoD contracts in accordance with the clause at FAR 52.225–26 (which cites to OMB 0704–0460). The information collection requirements for private security contractors under contracts with non-DoD agencies are addressed under a separate information collection, 9000–0180. There is no net impact of this final rule on the information collection requirements for OMB 0704–0460.

**List of Subjects in 48 CFR Parts 225 and 252**

Government procurement.

**Manuel Quinones,**  
*Editor, Defense Acquisition Regulations System.*

Therefore, 48 CFR parts 225 and 252 are amended as follows:

- 1. The authority citation for 48 CFR parts 225 and 252 continues to read as follows:

**Authority:** 41 U.S.C. 1303 and 48 CFR Chapter 1.

**PART 225—FOREIGN ACQUISITION**

**225.370 [Removed]**

- 2. Remove section 225.370.

**252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES**

**252.225–7039 [Removed and Reserved]**

- 3. Remove and reserve section 252.225–7039.

[FR Doc. 2013–27314 Filed 11–15–13; 8:45 am]

**BILLING CODE 5001–06–P**