DEPARTMENT OF DEFENSE

Defense Acquisition Regulations System

48 CFR Part 252

[Docket DARS–2015–0039]

RIN 0750–AI61

Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013–D018)

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 provide contractors with additional time to implement security requirements specified by a National Institute of Standards and Technology Special Publication.

DATES: *Effective date:* December 30, 2015.

Comment date: Comments on the interim rule should be submitted in writing to the address shown below on or before February 29, 2016 to be considered in the formation of a final rule.

ADDRESSES: Submit comments identified by DFARS Case 2013–D018, using any of the following methods:

- *Regulations.gov: http://www.regulations.gov.* Submit comments via the Federal eRulemaking portal by entering ''DFARS Case 2013–D018'' under the heading ''Enter keyword or ID'' and selecting ''Search.'' Select the link ''Submit a Comment'' that corresponds with ''DFARS Case 2013–D018.'' Follow the instructions provided at the ''Submit a Comment'' screen. Please include your name, company name (if any), and ''DFARS Case 2013–D018'' on your attached document.
- *Email: osd.dfars@mail.mil.* Include DFARS Case 2013–D018 in the subject line of the message.
- *Fax:* 571–372–6094.
- *Mail:* Defense Acquisition Regulations System, Attn: Mr. Dustin Pitsch, OUSD(AT&L)DPAP/DARS, Room 3B941, 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: Mr. Dustin Pitsch, telephone 571–372–6090.

SUPPLEMENTARY INFORMATION:

I. Background

DoD published an interim rule under this case number in the **Federal Register** (80 FR 51739) on August 26, 2015, to implement section 941 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013 (Pub. L. 112–239), section 1632 of the NDAA for FY 2015, and DoD policies and procedures with regard to cloud computing. The first interim rule expanded safeguarding requirements to cover the safeguarding of covered defense information, and required compliance with the security requirements in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, ''Protecting Controlled Unclassified Information in Nonfederal Information Systems and organizations,'' to replace the table based on NIST SP 800–53. The security requirements in NIST SP 800–171 are specifically tailored for use in protecting sensitive information residing in contractor information systems and generally reduce the burden placed on contractors by eliminating Federal-centric processes and requirements.

To address concerns from industry with regard to implementation of the first interim rule, DoD held a public meeting on Monday, December 14, 2015 (80 FR 72712, November 20, 2015). There were 85 registered attendees. Various topics were discussed with industry at the public meeting, such as scope, applicability, training, subcontractor flowdown, and implementation issues. Industry representatives specifically expressed to DoD, both prior to and at the public meeting, the need for additional time to implement the security requirements specified by NIST SP 800–171.

II. Discussion and Analysis

This second interim rule amends DFARS provision 252.204–7008, Compliance with Safeguarding and Covered Defense Information Controls, and DFARS clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, to provide offerors additional time to implement the security requirements specified by NIST SP 800–171, which will be required to be in place not later than December 31, 2017. The clause is also amended to require contractors to notify the DoD Chief Information Officer (CIO) of any NIST SP 800–171 security requirements that are not implemented at the time of contract award, within 30 days of contract award. The status provided by the contractor to the DoD CIO on implementation of the NIST SP 800–171 security requirements will enable the Department to monitor progress across the Defense industrial base, identify trends in the implementation of these requirements and, in particular, identify issues with industry implementation of specific requirements that may require clarification or adjustment. Additionally, this information will inform the Department in assessing the overall risk to DoD covered defense information on unclassified contractor systems and networks.

The second interim rule makes the following additional changes:

- The subcontractor flowdown requirements in DFARS provision 252.204–7009 and clause 252.204–7012 are amended to require, when applicable, inclusion of the clause without alteration, except to identify the parties.
- The subcontractor flowdown requirement in DFARS clause 252.204–7012 is further amended to limit the requirement to flow down the clause only to subcontractors where their efforts will involve covered defense information or where they will provide operationally critical support.
- DFARS clause 252.204–7012 is amended to remove the requirement for DoD CIO acceptance of alternative but equally effective security measures prior to award.

This rule is part of DoD's retrospective plan, completed in August 2011, under Executive Order 13563, ''Improving Regulation and Regulatory Review.'' DoD's full plan and updates can be accessed at: *http://www.regulations.gov/#!docketDetail;D=DOD-2011-OS-0036.*

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

DoD expects that the additional implementation period provided by this interim rule may have a significant beneficial economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act 5 U.S.C. 601, *et seq*. Therefore, an initial regulatory flexibility analysis has been prepared and is summarized as follows:

This rule allows contractors until December 31, 2017, to implement the security requirements specified by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, ''Protecting Controlled Unclassified Information in Nonfederal Information Systems and organizations,'' for safeguarding sensitive information residing in contractor information systems, contained in Defense Federal Acquisition Regulation Supplement clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

The objective of this rule is to allow contractors additional time to implement the security requirements necessary to improve protection for DoD information stored on or transiting contractor systems.

This rule will apply to all contractors with covered defense information transiting their information systems. DoD estimates that this rule may apply to 10,000 contractors and that less than half of those are small businesses.

This second interim rule requires contractors, within 30 days of contract award, to notify the DoD Chief Information Officer of any NIST SP 800–171 security requirements that are not implemented at the time of contract award. This new reporting requirement affects the existing information collection requirements approved under the first interim rule under OMB Control number 0704–0478, titled ''Enhanced Safeguarding and Cyber Incident Reporting of Unclassified DoD Information Within Industry,'' but the effect on the total burden hours is negligible.

The rule does not duplicate, overlap, or conflict with any other Federal rules.

No significant alternatives, that would minimize the economic impact of the rule on small entities, were determined.

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 2013–D018), in correspondence.

V. Paperwork Reduction Act

This rule affects the information collection requirements in the clause at DFARS 252.204–7012, currently approved under OMB Control Number 0704–0478, titled ''Enhanced Safeguarding and Cyber Incident Reporting of Unclassified DoD Information Within Industry,'' in accordance with the Paperwork Reduction Act (44 U.S.C. chapter 35). The impact, however, is negligible, because the new reporting requirement is not anticipated to increase the estimate of total burden hours.

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.

The proliferation of information technology and increased information access has exposed DoD and DoD contractor information systems and networks to greater vulnerability of attacks. The first interim rule under this case number and title was necessary because of the urgent need to protect covered defense information and gain awareness of the full scope of cyber incidents being committed against defense contractors. That rule addressed the requirement for contractors and subcontractors to report cyber incidents that result in an actual or potentially adverse effect on a covered contractor information system or covered defense information residing therein, or on a contractor's ability to provide operationally critical support. However, since issuance of the first interim rule, industry has expressed to DoD the need for additional time to implement one part of the first interim rule, specifically the NIST SP 800–171 security requirements for covered contractor information systems.

This second interim rule is being issued without the benefit of public comment to provide immediate relief from the requirement to have NIST 800–171 security requirements implemented at the time of contract award. Contractors are at risk of not being able to comply with the terms of contracts that require the handling of covered defense information. Contractors will be given until December 31, 2017 for implementation of the NIST 800–171 security requirements, thereby limiting the burden imposed on industry in the first interim rule. This rule grants additional time for contractors to assess their information systems and to set forth an economically efficient strategy to implement the new security requirements at a pace that fits within normal information technology lifecycle timelines. 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 Part 252

Government procurement.

Jennifer L. Hawes,

Editor, Defense Acquisition Regulations System.

Therefore, 48 CFR part 252 is amended as follows:

■ 1. The authority citation for 48 CFR part 252 continues to read as follows:

Authority: 41 U.S.C. 1303 and CFR chapter 1.

PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

■ 2. Amend section 252.204–7008 by—

■ a. Removing clause date ''(AUG 2015)'' and adding ''(DEC 2015)'' in its place;

■ b. Revising paragraph (c); and

■ c. Removing paragraph (d).

The revision reads as follows:

252.204–7008 Compliance with Safeguarding Covered Defense Information Controls.

* * * * *

(c) For covered contractor information systems that are not part of an information technology (IT) service or system operated on behalf of the Government (see 252.204–7012(b)(1)(ii))—

(1) By submission of this offer, the Offeror represents that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, ''Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations'' (see *http://dx.doi.org/10.6028/NIST.SP.800-171*), not later than December 31, 2017.

(2)(i) If the Offeror proposes to vary from any of the security requirements specified by NIST SP 800–171 that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer, the Offeror shall

submit to the Contracting Officer, for consideration by the DoD Chief Information Officer (CIO), a written explanation of—

(A) Why a particular security requirement is not applicable; or

(B) How an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection.

(ii) An authorized representative of the DoD CIO will adjudicate offeror requests to vary from NIST SP 800–171 requirements in writing prior to contract award. Any accepted variance from NIST SP 800–171 shall be incorporated into the resulting contract.

* * * * *

■ 3. Amend section 252.204–7009 by—

■ a. Removing clause date ''(AUG 2015)'' and adding ''(DEC 2015)'' in its place;

■ b. In paragraph (a), adding in alphabetical order a definition for ''Compromise''; and

■ c. Revising paragraph (c).

The addition and revision read as follows:

252.204–7009 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

* * * * *

(a) * * *

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.

* * * * *

(c) *Subcontracts.* The Contractor shall include this clause, including this paragraph (c), in subcontracts, or similar contractual instruments, for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial items, without alteration, except to identify the parties.

* * * * *

■ 4. Amend section 252.204–7012 by—

■ a. Removing clause date ''(SEP 2015)'' and adding ''(DEC 2015)'' in its place;

■ b. In paragraph (a), in the definition of ''Cyber incident,'' adding ''a compromise or'' after ''that result in'';

■ c. Revising paragraphs (b)(1)(ii)(A) and (B); and

■ d. Revising paragraphs (m)(1) and (2).

The revisions read as follows:

252.204–7012 Safeguarding Covered Defense Information and Cyber Incident Reporting.

* * * * *

(b) * * *

(1) * * *

(ii) * * *

(A) The security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, ''Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,'' *http://dx.doi.org/10.6028/NIST.SP.800-171* that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer, as soon as practical, but not later than December 31, 2017. The Contractor shall notify the DoD CIO, via email at *osd.dibcsia@mail.mil,* within 30 days of contract award, of any security requirements specified by NIST SP 800–171 not implemented at the time of contract award; or

(B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO; and

* * * * *

(m) * * *

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve a covered contractor information system, including subcontracts for commercial items, without alteration, except to identify the parties; and

(2) When this clause is included in a subcontract, require subcontractors to rapidly report cyber incidents directly to DoD at *http://dibnet.dod.mil* and the prime Contractor. This includes providing the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable.

* * * * *

[FR Doc. 2015–32869 Filed 12–29–15; 8:45 am]

BILLING CODE 5001–06–P