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.

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.
239.7300 Scope of subpart.
239.7301 Applicability.
239.7302 Definitions.
239.7303 Authorized individuals.
239.7304 Determination and notification.
239.7305 Exclusion and limitation on disclosure.
239.7306 Solicitation provision and contract clause.

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