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

AGENCIES: 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 **[Insert 60 days after publication in the FEDERAL REGISTER]** 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 websites.
  - 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.
4.1700 Scope of subpart.
4.1701 Definitions.
4.1702 Applicability.
4.1703 Solicitation provision and contract clause.

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 websites: 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 websites 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 website 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.

[BILLING CODE 6820-EP]

[FR Doc. 2012-20881 Filed 08/23/2012 at 8:45 am; Publication Date: 08/24/2012]