Dated: June 17, 2011.

Mark S. Ogle,

Captain, U.S. Coast Guard Captain of the Port Hampton Roads.

[FR Doc. 2011–16345 Filed 6–28–11; 8:45 am]

BILLING CODE 9110–04–P

DEPARTMENT OF DEFENSE

GENERAL SERVICES ADMINISTRATION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

48 CFR Parts 2, 3, 4, 7, 9, 11, 12, 13, 14, 15, 16, 18, 37, 42, 52, and 53

[FAR Case 2011–001; Docket 2011–0001; Sequence 1]

RIN 9000–AL82

Federal Acquisition Regulation; Organizational Conflicts of Interest

AGENCY: Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA).

ACTION: Proposed rule; reopening of comment period.

SUMMARY: DoD, GSA, and NASA are proposing to amend the Federal Acquisition Regulation (FAR) to provide revised regulatory coverage on organizational conflicts of interest (OCIs), provide additional coverage regarding contractor access to nonpublic information, and add related provisions and clauses. Section 841 of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 required a review of the FAR coverage on OCIs. This proposed rule was developed as a result of a review conducted in accordance with Section 841 by the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council (the Councils) and the Office of Federal Procurement Policy (OFPP), in consultation with the Office of Government Ethics (OGE). This proposed rule was preceded by an Advance Notice of Proposed Rulemaking (ANPR), under FAR Case 2007–018 (73 FR 15962), to gather comments from the public with regard to whether and how to improve the FAR coverage on OCIs. The comment period is being reopened for an additional 30 days to provide additional time for interested parties to review the proposed FAR changes.

DATES: The comment period for the proposed rule that published on April 26, 2011 at 76 FR 23236 is reopened. Interested parties should submit written comments to the Regulatory Secretariat at one of the addressees shown below on or before July 27, 2011 to be considered in the formation of the final rule.

ADDRESSES: Submit comments in response to FAR case 2011–001 by any of the following methods:

- *Regulations.gov: http://www.regulations.gov.* Submit comments via the Federal eRulemaking portal by inputting ''FAR Case 2011–001'' under the heading ''Enter Keyword or ID'' and selecting ''Search.'' Select the link ''Submit a Comment'' that corresponds with ''FAR Case 2011–001.'' Follow the instructions provided at the ''Submit a Comment'' screen. Please include your name, company name (if any), and ''FAR Case 2011–001'' 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 2011–001, in all correspondence related to this case. All comments received will be posted without change to *http://www.regulations.gov,* including any personal and/or business confidential information provided.

FOR FURTHER INFORMATION CONTACT: Mr. Anthony Robinson, Procurement Analyst, at (202) 501–2658, for clarification of content. For information pertaining to status or publication schedules, contact the Regulatory Secretariat at (202) 501–4755. Please cite FAR Case 2011–001.

SUPPLEMENTARY INFORMATION:

Background

The Councils published a proposed rule in the **Federal Register** at 76 FR 23236, April 26, 2011. The comment period is being reopened for an additional 30 days to provide additional time for interested parties to review the proposed FAR changes. Therefore, accordingly, the comment period for the proposed rule that published on April 26, 2011 at 76 FR 23236 is reopened.

Dated: June 23, 2011.

Millisa Gary,

Acting Director, Federal Acquisition Policy Division.

[FR Doc. 2011–16338 Filed 6–28–11; 8:45 am]

BILLING CODE 6820–EP–P

DEPARTMENT OF DEFENSE

Defense Acquisition Regulations System

48 CFR Parts 204 and 252

RIN 0750–AG47

Defense Federal Acquisition Regulation Supplement; Safeguarding Unclassified DoD Information (DFARS Case 2011–D039)

AGENCY: Defense Acquisition Regulations System, Department of Defense (DoD).

ACTION: Proposed rule.

SUMMARY: DoD is proposing to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to add a new subpart and associated contract clauses to address requirements for safeguarding unclassified DoD information.

DATES: Comments on the proposed rule should be submitted in writing to one of the addresses shown below on or before August 29, 2011, to be considered in the formation of the final rule.

ADDRESSES: Submit comments identified by DFARS Case 2011–D039, using any of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *E-mail: dfars@osd.mil.* Include DFARS Case 2011–D039 in the subject line of the message.
- *Fax:* 703–602–0350.
- *Mail:* Defense Acquisition Regulations System, *Attn:* Mr. Julian Thrash, 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, please check *http://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. Julian Thrash, telephone 703–602–0310.

SUPPLEMENTARY INFORMATION:

I. Background

The DFARS does not presently address the safeguarding of unclassified DoD information within industry, nor does it address cyber intrusion reporting for that 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, to provide the public an opportunity for input into the initial rulemaking process. The ANPR addressed basic and enhanced safeguarding procedures for the protection of DoD information.

The purpose of this proposed DFARS rule is 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. This rule addresses the safeguarding requirements specified in Executive Order 13556, Controlled Unclassified Information. On-going efforts, currently being led by the National Archives and Records Administration regarding controlled unclassified information, may also require future DFARS revisions in this area. This case does not address procedures for Government sharing of cyber security threat information with industry; this issue will be addressed separately through follow-on rulemaking procedures as appropriate.

This proposed rule addresses basic and enhanced safeguarding requirements, including cyber incident reporting, that apply to information subject to the following for information—

- Designated as critical program information in accordance with DoD Instruction 5200.39, Critical Program Information (CPI) Protection Within the Department of Defense, at *http://www.dtic.mil/whs/directives/corres/pdf/520039p.pdf;*
- Designated as critical information in accordance with DoD Directive 5205.02, DoD Operations Security (OPSEC) Program, at *http://www.dtic.mil/whs/directives/corres/pdf/520502p.pdf;*
- Subject to export controls under International Traffic in Arms Regulations and Export Administration Regulations;
- Exempt from mandatory public disclosure under DoD Directive 5400.07, DoD Freedom of Information Act (FOIA) Program, at *http://www.dtic.mil/whs/directives/corres/pdf/540007p.pdf*, and DoD Regulation 5400.7–R, DoD Freedom of Information Program, at *http://www.dtic.mil/whs/directives/corres/pdf/540007r.pdf*;
- Bearing current and prior designations indicating controlled access and dissemination (e.g., For Official Use Only, Sensitive But Unclassified, Limited Distribution, Proprietary, Originator Controlled, Law Enforcement Sensitive);
- That 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*; or
- That is personally identifiable information including, but not limited to, information protected pursuant to the Privacy Act and the Health Insurance Portability and Accountability Act.

The proposed DFARS changes would revise the clause at DFARS 252.204–7000, Disclosure of Information, to add a definition of ''DoD information,'' and ''nonpublic information.'' This case also proposes to add two new clauses—

- DFARS 252.204–70XX, Basic Safeguarding of Unclassified DoD Information; and
- DFARS 252.204–70YY, Enhanced Safeguarding of Unclassified DoD Information.

DFARS 252.204–70XX, Basic Safeguarding of Unclassified DoD Information, would require the implementation of first-level protection measures for the protection of Government information; with the point to deter unauthorized disclosure, loss, or exfiltration by employing first-level information technology security measures.

DFARS 252.204–70YY Enhanced Safeguarding of Unclassified DoD Information, would require enhanced information technology security measures applicable to the encryption of data for storage and transmission, network protection and intrusion detection, and cyber intrusion reporting. A cyber intrusion reporting requirement is planned for enhanced protection to assess the impact of loss and improve protection by better understanding the methods of loss.

II. Executive Orders 12861 and 13563

Executive Orders 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). Executive Order 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

DoD expects that this proposed rule may have an 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 (IRFA) has been prepared and is summarized as follows.

The objective of this rule is for DoD to avoid compromise of unclassified computer networks on which DoD information is resident on or transiting through contractor information systems, and to prevent the exfiltration of DoD information on such systems. The benefit of tracking and reporting DoD incursions is to—

- Assess the impact of loss;
- Better understand methods of loss;
- Facilitate information sharing and collaboration; and
- Standardize procedures for tracking and reporting intrusions.

This proposed rule requires a basic and an enhanced level of information protection. For the basic protection, the resultant cost impact is considered to not be 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 an enormous detriment to contractor and DoD business, resulting in reduced system performance, and the potential loss of valuable information. It is also recognized that prudent business practices to protect an information technology system are typically a common part of everyday operations. As a result, the benefit of securely receiving and processing unclassified DoD information offers enormous value to contractors and DoD by reducing vulnerabilities to contractor systems by keeping unclassified DoD information from being exfiltrated.

DoD requires an enhanced level of information assurance planning, including reporting of information loss or cyber-intrusions for DoD contractors that handle DoD unclassified information that has special handling requirements for critical program information. This requirement would also be passed down through the supply chain. DoD believes that most

information passed down the supply chain will not require special handling and recognizes that most large contractors handling sensitive information already have sophisticated information assurance programs and can take credit for existing controls with minimal additional cost. However, most non-large businesses have less sophisticated programs and will realize costs meeting the additional requirements.

DoD estimates that the rule will apply to approximately 76 percent of DoD's small business contractors in that they will be required to provide protection of DoD information at the enhanced level. DoD awarded contracts to 64,427 businesses with unique parent Data Universal Numbering System identified as small businesses in fiscal year 2010, so the estimated impact of this rule is to 48,965 unique small businesses. Additionally, a reasonable rule of thumb for small businesses is that information technology security costs are approximately 0.5 percent of total revenues. Because there are economies of scale when it comes to information security, larger businesses generally pay only a fraction of that estimated cost as a percentage of total revenue.

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 2011–D039) in correspondence.

IV. Paperwork Reduction Act

The Paperwork Reduction Act (44 U.S.C. Chapter 35) applies because the proposed rule does contain information collection requirements. DoD invites comments on the following aspects of the proposed rule: (a) Whether the collection of information is necessary for the proper performance of the functions of DoD, including whether the information will have practical utility; (b) the accuracy of the estimate of the burden of the information collection; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the information collection on respondents, including the use of automated collection techniques or other forms of information technology.

The following is a summary of the information collection requirement.

Title: Defense Federal Acquisition Regulation Supplement; Safeguarding of Unclassified Information.

Type of Request: New collection.

Number of Respondents: 65,728.

Responses per Respondent: Approximately 0.5

Annual Responses: 32,864.

Average Burden per Response: 1 hour.

Annual Burden Hours: 32,864.

Needs and Uses: DoD needs the information required by 252.204–70YY in order to properly track cyber incident reporting of unclassified information within industry.

Affected Public: Businesses or other for-profit institutions.

Respondent's Obligation: Required to obtain or retain benefits.

Frequency: On occasion.

Written comments and recommendations on the proposed information collection should be sent to Ms. Jasmeet Seehra at the Office of Management and Budget, Desk Officer for DoD, Room 10236, New Executive Office Building, Washington, DC 20503, with a copy to the Defense Acquisition Regulations System, Attn: Mr. Julian Thrash, OUSD (AT&L) DPAP/DARS, Room 3B855, 3060 Defense Pentagon, Washington, DC 20301–3060. Comments can be received from 30 to 60 days after the date of this notice, but comments to OMB will be most useful if received by OMB within 30 days after the date of this notice.

To request more information on this proposed information collection or to obtain a copy of the proposal and associated collection instruments, please write to the Defense Acquisition Regulations System, *Attn:* Mr. Julian Thrash, OUSD (AT&L) DPAP/DARS, Room 3B855, 3060 Defense Pentagon, Washington, DC 20301–3060.

List of Subjects in 48 CFR Parts 204 and 252

Government procurement.

Mary Overstreet,

Editor, Defense Acquisition Regulations System.

Therefore, DoD proposes to amend 48 CFR parts 204 and 252 as follows:

1. The authority citation for 48 CFR parts 204 and 252 continues to read as follows:

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

PART 204–ADMINISTRATIVE MATTERS

2. Add subpart 204.74 to read as follows:

Subpart 204.74—Safeguarding Unclassified DoD Information

Subpart 204.74—Safeguarding Unclassified DoD Information

204.7400 Scope.

(a) This subpart applies to contracts and subcontracts requiring basic and enhanced safeguarding of unclassified DoD information resident on or transiting through contractor information systems.

(b) This subpart does not apply to voice information.

(c) This subpart does not abrogate any existing contractor physical, personnel, or general administrative security operations governing the protection of unclassified DoD information, nor does it apply to or impact upon contractors' National Industrial Security Program.

204.7401 Definitions.

As used in this subpart—

Adequate security is defined in the clause at 252.204–70XX, Basic Safeguarding of Unclassified DoD Information.

Cyber is defined in the clause at 252.204–70YY, Enhanced Safeguarding of Unclassified DoD Information.

DoD information and *nonpublic information* are defined in the clause at 252.204–7000, Disclosure of Information.

204.7402 Policy.

(a) The Government and its contractors and subcontractors will provide adequate security to safeguard unclassified DoD information on their unclassified information systems from unauthorized access and disclosure.

(b) Contractors must report to the Government certain cyber incidents that affect unclassified DoD information resident on or transiting contractor unclassified information systems. Detailed reporting criteria and requirements are set forth in the clause at 252.204–70YY.

(c) A cyber incident that is properly reported by the contractor shall not, by itself, be interpreted as evidence that the contractor has failed to provide adequate information safeguards for DoD unclassified information, or has otherwise failed to meet the requirements of the clause at 252.204–70YY. Contracting officers shall consult with a functional manager to assess contract performance. A cyber incident will be evaluated in context, and such events may occur even in cases when it is determined that adequate safeguards are being used in view of the nature and sensitivity of the DoD unclassified

information and the anticipated threats. However, the Government may consider any such cyber incident in the context of an overall assessment of the contractor's compliance with the requirements of the clause at 252.204–70YY.

(d) DoD information may require—

(1) Basic safeguarding requirements, as specified in clause 252.204–70XX, apply to any DoD information; and

(2) Enhanced safeguarding requirements, including cyber incident reporting as specified in clause 252.204.70YY, apply to DoD information that is—

(i) Designated as Critical Program Information in accordance with DoD Instruction 5200.39, Critical Program Information Protection Within the Department of Defense;

(ii) Designated as critical information in accordance with DoD Directive 5205.02, DoD Operations Security (OPSEC) Program;

(iii) Subject to export control under International Traffic in Arms Regulations and Export Administration Regulations (see subpart 204.73);

(iv) Exempt from mandatory public disclosure under DoD Directive 5400.07, DoD Freedom of Information Act (FOIA) Program, and DoD Regulation 5400.7–R, DoD Freedom of Information Program;

(v) Bearing current and prior designations indicating controlled access and dissemination (e.g., For Official Use Only, Sensitive But Unclassified, Limited Distribution, Proprietary, Originator Controlled, Law Enforcement Sensitive);

(vi) Technical data, computer software, and any other technical information covered by DoD Directive 5230.24, Distribution Statements on Technical Documents, and DoD Directive 5230.25, Withholding of Unclassified Technical Data from Public Disclosure; or

(vii) Personally identifiable information including, but not limited to, information protected pursuant to the Privacy Act and the Health Insurance Portability and Accountability Act.

204.7403 Procedures.

The contracting officer shall receive input from the requirements office, which will determine information controls for access and distribution (follow the procedures at PGI 204.74).

204.7404 Contract clauses.

(a) Use the clause at 252.204–70XX, Basic Safeguarding of Unclassified DoD Information, in solicitations and contracts when the requiring activity has identified that the contractor or a subcontractor at any tier will potentially have unclassified DoD information resident on or transiting through its unclassified information systems; and

(b) Use the clause at 252.204–70YY, Enhanced Safeguarding of Unclassified DoD Information, in solicitations and contracts when the requiring activity has identified that the contractor or a subcontractor at any tier will potentially have unclassified DoD information resident on or transiting through its unclassified information systems that requires an enhanced level of protection.

PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

3. Section 252.204–7000 is revised to read as follows:

252.204–7000 Disclosure of Information.

As prescribed in 204.404–70(a), use the following clause:

DISCLOSURE OF INFORMATION (DATE)

(a) *Definitions.* As used in this clause—

DoD information means any nonpublic information that—

(1) Has not been cleared for public release in accordance with DoD Directive 5230.09, Clearance of DoD Information for Public Release; and

(2) Is—

(i) Provided by or on behalf of the Department of Defense (DoD) to the Contractor or its subcontractor(s); or

(ii) Collected, developed, received, transmitted, used, or stored by the Contractor or its subcontractor(s) in support of an official DoD activity.

Nonpublic information means any Government or third-party information that–

(1) Is exempt from disclosure under the Freedom of Information Act (5 U.S.C. 552) or otherwise protected from disclosure by statute, Executive order, or regulation; or

(2) Has not been disseminated to the general public, and the Government has not yet determined whether the information can or will be made available to the public.

(b) The Contractor shall not release any unclassified DoD information to anyone outside the Contractor's organization any unclassified information, or any employee inside the Contractor's organization without a need-to-know, regardless of medium (e.g., film, tape, document), pertaining to any part of this contract or any program related to this contract, unless—

(1) This information is required—

(i) As part of an official Defense Contract Audit Agency audit;

(ii) By DoD Offices of the Inspector General as part of pending or on-going investigations; or

(iii) By a Congressional or Federal (Department of Justice) subpoena.

(2) The information is otherwise in the public domain before the date of release; or

(3) This information results from or arises during the performance of a project that has been scoped, negotiated, and determined to be fundamental research within the definition of National Security Decision Directive 189 according to the prime contractor and research performer and certified by the contracting component, and that is not subject to restrictions due to classification, except as otherwise required by applicable Federal statutes, regulations, or Executive orders.

(c) Requests for approval shall identify the specific DoD information to be released, the medium to be used, and the purpose for the release. The Contractor shall submit its request to the Contracting Officer at least 45 days before the proposed date for release.

(d) The Contractor agrees to include a similar requirement in each subcontract under this contract. Subcontractors shall submit requests for authorization to release through the prime contractor to the Contracting Officer.

4. Add sections 252.204–70XX and 252.204–70YY as follows:

252.204–70XX Basic Safeguarding of Unclassified DoD Information.

As prescribed in 204.7404(a), use the following clause:

BASIC SAFEGUARDING OF UNCLASSIFIED DOD INFORMATION (DATE)

(a) *Definitions.* As used in this clause—

Adequate security means protective measures are applied commensurate with the risks (i.e., consequences and their probability) of loss, misuse, or unauthorized access to or modification of information.

Clearing information means a level of media sanitization that would protect the confidentiality of information against a robust keyboard attack. Simple deletion of items would not suffice for clearing. For example, overwriting is an acceptable method for clearing media. The security goal of the overwriting process is to replace written data with random data.

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.

Data means a subset of information in an electronic format that allows it to be retrieved or transmitted.

DoD information is defined in the clause 252.204–7000, Disclosure of Information.

Exfiltration means any unauthorized release of data from within an information system. This includes copying the data through covert network channels or the copying of data to unauthorized media.

Government information means any unclassified nonpublic information that is—

(1) Provided by or on behalf of the Government to the contractor or its subcontractor(s); or

(2) Collected, developed, received, maintained, disseminated, transmitted, used, or stored by the Contractor or its subcontractor(s) in support of an official Government activity.

Information means any communicable knowledge or documentary material, regardless of its physical form or characteristics.

Information system means a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information.

Intrusion means unauthorized access to an information system, such as an act of entering, seizing, or taking possession of another's property to include electromagnetic media.

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 onto which information is recorded, stored, or printed within an information system.

Nonpublic information is defined in the clause 252.204–7000, Disclosure of Information.

Safeguarding means measures and controls that are used to protect DoD information.

Threat means any person or entity that attempts to access or accesses an information system without authority.

Voice means all oral information regardless of transmission protocol.

(b) *Safeguarding requirements and procedures.* The Contractor shall provide adequate security to safeguard unclassified Government information on its unclassified information systems from unauthorized access and disclosure. The Contractor shall apply the following basic safeguarding requirements to Government information:

(1) *Protecting unclassified Government information on public computers or websites:* Do not process unclassified Government 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. Unclassified Government 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 (vice the website itself or the application it hosts).

(2) *Transmitting electronic information.* Transmit email, text messages, blogs, and similar communications 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 voice and fax information only when the sender has a reasonable assurance that access is limited to authorized recipients.

(4) *Physical or electronic barriers.* Protect information by at least one physical or 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 has been used to process unclassified Government 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 least the following protections against computer intrusions and data compromise including exfiltration:

(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 Government information only to those subcontractors that both have a need to know 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 potentially have unclassified Government information resident on or transiting through their unclassified information systems.

(End of clause)

252.204–70YY Enhanced Safeguarding of Unclassified DoD Information.

As prescribed in 204.7404(b), use the following clause:

ENHANCED SAFEGUARDING OF UNCLASSIFIED DOD INFORMATION (DATE)

(a) *Definitions.* As used in this clause—

Adequate security is defined in the clause 252.204–70XX, Basic Safeguarding of Unclassified DoD Information.

Attribution information means information that identifies the Contractor or its programs, whether directly or indirectly, by the aggregation of information that can be traced back to the Contractor (e.g., program description, facility locations, number of personnel).

Authentication means the process of verifying the identity or other attributes claimed by or assumed of an entity, or to verify the source and integrity of data.

Compromise is defined in the clause 252.204–70XX, Basic Safeguarding of Unclassified DoD Information.

Contractor information system means an information system belonging to, or operated by or for, the Contractor or a subcontractor.

Critical Program Information means elements or components of a research, development, or acquisition program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability. The term includes information about applications, capabilities, processes, and end items; elements or components critical to a military system or network mission effectiveness; and technology that would reduce the U.S. technological advantage if it came under foreign control.

Cyber means of, relating to, or involving computers or computer networks.

Data means a subset of information in an electronic format that allows it to be retrieved or transmitted.

DoD information is defined in the clause 252.204–7000, Disclosure of Information.

Exfiltration, Information and *Information system* are defined in the clause 252.204–70XX, Basic Safeguarding of Unclassified DoD Information.

Incident means unauthorized access to an information system, such as an act of entering, seizing, or taking possession of another's property to include electromagnetic media.

Intrusion, Media, Safeguarding and *Threat* are defined in the clause 252.204–70XX, Basic Safeguarding of Unclassified DoD Information.

(b) *Safeguarding requirements and procedures.* The Contractor shall provide adequate security to safeguard unclassified DoD information on its information systems from unauthorized access and disclosure. Adequate security includes—

(1) Safeguarding all unclassified DoD information in accordance with the basic requirements set forth in DFARS clause 252.204–70XX, Basic Safeguarding of Unclassified DoD Information;

(2) Safeguarding DoD information described in paragraph (c) of this clause in accordance with—

(i) The enhanced safeguarding requirements, as a minimum, in paragraph (d) of this clause; and

(ii) The Contractor shall apply other information security requirements when the Contractor reasonably determines that information security measures, in addition to those identified in paragraph (b)(1) and (b)(2)(i) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

(c) *DoD information requiring enhanced safeguarding.* Enhanced safeguarding requirements, including cyber incident reporting, apply to DoD information that is—

(1) Designated as Critical Program Information in accordance with DoD Instruction 5200.39, Critical Program Information (CPI) Protection Within the Department of Defense;

(2) Designated as critical information in accordance with DoD Directive 5205.02, DoD Operations Security (OPSEC) Program;

(3) Subject to export controls under International Traffic in Arms Regulations and Export Administration Regulations;

(4) Exempt from mandatory public disclosure under DoD Directive 5400.07, DoD Freedom of Information Act (FOIA) Program, and DoD Regulation 5400.7–R, DoD Freedom of Information Program;

(5) Bearing current and prior designations indicating controlled access and dissemination (e.g., For Official Use Only, Sensitive But Unclassified, Limited Distribution, Proprietary, Originator Controlled, Law Enforcement Sensitive);

(6) Technical data, computer software, and any other technical information covered by DoD Directive 5230.24, Distribution Statements on Technical Documents, and

DoD Directive 5230.25, Withholding of Unclassified Technical Data from Public Disclosure; or

(7) Personally identifiable information including, but not limited to, information protected pursuant to the Privacy Act and the Health Insurance Portability and Accountability Act.

(d) *Enhanced safeguarding requirements.* (1) The Contractor shall apply the following safeguarding requirements for DoD information that requires enhanced safeguarding:

(2) The Contractor shall implement information security in its project, enterprise, or company-wide unclassified information technology system(s). The information security program shall implement, at a minimum, the specified National Institute of Standards and Technology (NIST) Special Publication (SP) 800–53 security controls identified in paragraph (d)(3) of this Enhanced Safeguarding clause of this contract, or, if the control is not implemented, the Contractor shall prepare a written determination that explains how either the required security control identified in paragraph (d)(3) of this clause is not applicable, or how an alternative control or protective measure is used to achieve equivalent protection. The Contractor shall provide the written determination to the Contracting Officer upon request. A description of the security controls is in the NIST SP 800–53 (current version at time of award), ''Recommended Security Controls for Federal Information Systems and Organizations'' (*http://csrc.nist.gov/publications/PubsSPs.html*).

(3) The NIST SP 800–53 (current version at time of award) security controls identified in Table 1 of this clause provide a minimum level of enhanced safeguarding for unclassified DoD Information. The Contractor shall implement these controls in accordance with paragraph (d)(2) and Table 1. Tailoring in scope and depth appropriate to the effort may be used as authorized in the contract.

TABLE 1—MINIMUM SECURITY CONTROLS FOR ENHANCED SAFEGUARDING MINIMUM REQUIRED SECURITY CONTROLS FOR DOD INFORMATION REQUIRING ENHANCED SAFEGUARDING IN ACCORDANCE WITH PARAGRAPH (b)(2) OF THE ENHANCED SAFEGUARDING CLAUSE OF THIS CONTRACT (REFERENCE NIST SP 800–53, ''RECOMMENDED SECURITY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS'')

Access control	Awareness & training	Contingency planning	Maintenance	System & comm protection
AC–2	AT–2	CP–9	MA–4	SC–2.
AC–3			MA–4(6)	SC–4.
AC–3(4)	Audit & Accountability	Identification and Authentication.	MA–5	SC–7.
AC–4	AU–2		MA–6	SC–7(2).
AC–6	AU–3	IA–2		SC–9.
AC–7	AU–6	IA–4	Media Protection	SC–9(1).
AC–11	AU–6(1)	IA–5	MP–4	SC–13.
AC–11(1)	AU–7	IA–5(1)	MP–6	SC–13(1).
AC–17	AU–8			SC–13(4).
AC–17(2)	AU–9	Incident Response	Physical and Environmental Protection.	SC–15.
AC–18	AU–10			SC–28.
AC–18(1)	AU–10(5)	IR–2	.	
AC–19		IR–4	PE–5	System & Information Integrity.
	Configuration Management	IR–5	PE–7	SI–2.
		IR–6		SI–3.
	CM–2		Program Management	SI–4.
	CM–6			
	CM–7		PM–10	
	CM–8			

Legend: AC: Access Control, AT: Awareness and Training, AU: Auditing and Accountability Protection, CM: Configuration Management, CP: Contingency Planning Acquisition, IA: Identification and Authentication Communications Protection, IR: Incident Response Integrity, MA: Maintenance, MP: Media Protection, PE: Physical & Environmental, PM: Program Management, SA: System and Services, SC: System, & SI: System & Information.

(4) *Authentication to DoD Information Systems.* In addition to the NIST SP 800–53 security control requirements for authentication, Contractor personnel will procure and use only DoD-approved identity authentication credentials for authentication to DoD information systems. Information system owners/operators will identify all appropriate DoD-approved identity credentials that can be used for authentication to an information system.

(e) *Other requirements.* This clause does not relieve the Contractor of the requirements specified by other Federal and DoD safeguarding requirements for categories of information (e.g., Critical Program Information, Operations Security, International Traffic in Arms Regulations, Export Administration Regulations, Freedom of Information Act, For Official Use Only, Sensitive But Unclassified, Limited Distribution, Proprietary, Originator Controlled, Law Enforcement Sensitive, Personally Identifiable Information, Privacy Act, and Health Insurance Portability and Accountability Act), as specified by applicable regulations or directives.

(f) *Cyber incident reporting.* (1) *Reporting requirement.* The Contractor shall report to DoD (URL to be determined) within 72 hours of discovery of any cyber incident, in accordance with paragraph (f)(2), that affects DoD information resident on or transiting through the Contractor's unclassified information systems.

(2) *Reportable cyber incidents.* Reportable cyber incidents include the following:

(i) A cyber incident involving possible data exfiltration or manipulation or other loss or compromise of any DoD information resident on or transiting through its, or its subcontractors', unclassified information systems.

(ii) Incident activities not included in paragraph (f)(2)(i) or (ii) of this clause that allow unauthorized access to an unclassified information system on which DoD 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., Critical Program Information, Operations Security, International Traffic in Arms Regulations, Export Administration Regulations, Freedom of Information Act, For Official Use Only, Sensitive But Unclassified, Limited Distribution, Proprietary, Originator Controlled, Law Enforcement Sensitive, Personally Identifiable Information, Privacy Act, and Health Insurance Portability and Accountability Act).

(4) *Contents of the cyber incident report.* The Contractor shall report the cyber incident to DoD using the incident form available at the following DoD URL: (URL to be determined).

(5) *Contractor actions to support forensic analysis and preliminary damage assessment.* In response to the reported cyber incident, the Contractor shall—

(i) Conduct an immediate review of its unclassified network for evidence of intrusion 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 initial compromise, as well as other information systems on the network that were accessed as a result of the initial compromise.

(ii) Review the data accessed during the cyber incident to identify specific DoD information associated with DoD programs, systems or contracts, including military programs, systems and technology.

(iii) The Contractor shall preserve and protect images of known affected information systems and all relevant monitoring/packet capture data until DoD has received the image and completes its analysis, or declines interest.

(iv) Cooperate with the DoD Damage Assessment Management Office (DAMO) to identify systems compromised as a result of the incident.

(v) Provide points of contact to coordinate damage assessment activities.

(6) *Damage assessment activities.* DAMO may conduct a damage assessment. If it is determined that the incident requires a damage assessment, DAMO will notify the Contractor to provide digital media and a point of contact to coordinate future damage assessment activities. The Contractor shall comply with DAMO information requests.

(g) *Protection of reported information.* Except to the extent that such information is publicly available, DoD will protect information reported or otherwise provided to DoD under this clause in accordance with applicable statutes, regulations, and policies (e.g., Critical Program Information, Operations Security, International Traffic in Arms Regulations, Export Administration Regulations, Freedom of Information Act, For Official Use Only, Sensitive But Unclassified, Limited Distribution, Proprietary, Originator Controlled, Law Enforcement Sensitive, Personally Identifiable Information, Privacy Act, and Health Insurance Portability and Accountability Act).

(1) The Contractor and its subcontractors shall mark attribution information reported or otherwise provided to the Government. The Government may use attribution information and disclose it only to authorized persons for cyber security and related purposes and activities pursuant to this clause (e.g., in support of forensic analysis, incident response, compromise or damage assessments, law enforcement, counterintelligence, threat reporting, trend analyses). Attribution information is shared outside of DoD only to authorized entities on a need-to-know basis as required for such Government cyber security and related activities. The Government may disclose attribution information to support contractors that are supporting the Government's cyber security and related activities under this clause only if the support contractor is subject to legal confidentiality requirements that prevent any further use or disclosure of the attribution information.

(2) The Government may use and disclose reported information that does not include attribution information (e.g., information regarding threats, vulnerabilities, incidents, or countermeasures at its discretion to assist entities in protecting information or information systems (e.g., threat information products, threat assessment reports); provided that such use or disclosure is otherwise authorized in accordance with applicable statutes, regulations, and policies.

(h) Nothing in this clause limits the Government's ability to conduct law enforcement or counterintelligence activities, or other lawful activities in the interest of 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.

(i) *Third party information.* If providing or sharing information is barred by the terms of a nondisclosure agreement with a third party, the Contractor will seek written permission from the owner of any third-party data believed to be contained in images or media that may be shared with the Government. Absent the written permission, the third-party information owner may have the right to pursue legal action against the Contractor (or its subcontractors) with access to the nonpublic information for breach or unauthorized disclosure.

(j) *Subcontracts.* The Contractor shall include the substance of this clause, including this paragraph (j), in all subcontracts under this contract that may have unclassified DoD information that requires enhanced protection. In altering this clause to identify the appropriate parties, the Contractor shall modify the reporting requirements to include notification to the prime Contractor or the next higher tier in addition to the reports to the DoD as required by paragraph (f) of this clause.

(End of clause)

[FR Doc. 2011–16399 Filed 6–28–11; 8:45 am]

BILLING CODE 5001–08–P

DEPARTMENT OF THE INTERIOR

Fish and Wildlife Service

50 CFR Part 17

[Docket No. FWS–R5–ES–2011–0024; MO 92210–0–0008]

Endangered and Threatened Wildlife and Plants; 90-Day Finding on a Petition To List the Eastern Small-Footed Bat and the Northern Long-Eared Bat as Threatened or Endangered

AGENCY: Fish and Wildlife Service, Interior.

ACTION: Notice of petition finding and initiation of status review.

SUMMARY: We, the U.S. Fish and Wildlife Service (Service), announce a 90-day finding on a petition (Petition) to list the eastern small-footed bat (*Myotis leibii*) and the northern long-eared bat (*Myotis septentrionalis*) as endangered or threatened under the Endangered Species Act of 1973, as amended (Act), and designate critical habitat. Based on our review, we find that the Petition presents substantial scientific or commercial information indicating that listing of the eastern small-footed bat and the northern long-eared bat may be warranted. Therefore, with the publication of this notice, we are initiating a review of the status of these species to determine if listing the eastern small-footed bat or the northern long-eared bat, or both species is warranted. To ensure that this status review is comprehensive, we are requesting scientific and commercial data and other information regarding these species. Based on the status review, we will issue a 12-month finding on the Petition, which will address whether the petitioned action is warranted, as provided in the Act.

DATES: To allow us adequate time to conduct this review, we request that we receive information on or before August 29, 2011. Please note that if you are using the Federal eRulemaking Portal (see **ADDRESSES**), the deadline for submitting an electronic comment is Eastern Standard Time on this date. After August 29, 2011, you must submit information directly to the Field Office (see **FOR FURTHER INFORMATION CONTACT**). Please note that we might not be able to address or incorporate information that we receive after the above requested date.

ADDRESSES: You may submit comments by one of the following methods:

Electronically: Go to the Federal eRulemaking Portal: *http://www.regulations.gov.* In the Keyword box, enter Docket No. FWS–R5–ES–2011–0024, which is the docket number for this finding. Follow the instructions for submitting comments on this docket.

By hard copy: Submit by U.S. mail or hand-delivery to: Public Comments Processing, Attn: FWS–R5–ES–2011–0024; Division of Policy and Directives Management; U.S. Fish and Wildlife Service; 4401 N. Fairfax Drive, MS 2042–PDM; Arlington, VA 22203.

We will not accept e-mails or faxes. We will post all information we receive on *http://www.regulations.gov.* This generally means that we will post any personal information you provide us, See Request for Information below for more information.