Flooding source(s)	Location of referenced elevation **	* Elevation in feet (NGVD) + Elevation in feet (NAVD) # Depth in feet above ground ∧ Elevation in meters (MSL)		Communities affected
		Effective	Modified	
	Approximately 25 feet downstream of East Concord Drive.	None	+901	
Dicks Creek	Approximately 20 feet upstream of the City of Trimble corporate limit.	None	+931	City of Trimble, Unincorporated Areas of Clinton County.
Funkhouser Creek	Approximately 725 feet downstream of the confluence with Concord Creek.	None	+876	City of Plattsburg.
	Approximately 350 feet downstream of the confluence with Concord Creek.	None	+878	
Funkhouser Creek	Approximately 225 feet upstream of Broadway Street	None	+923	City of Plattsburg, Unincorporated Areas of Clinton County.
	Approximately 25 feet downstream of Plotsky Avenue	None	+943	
Smithland Lake	Entire shoreline	None	+876	City of Trimble, Unincorporated Areas of Clinton County.

* National Geodetic Vertical Datum.
+ North American Vertical Datum.
# Depth in feet above ground.
∧ Mean Sea Level, rounded to the nearest 0.1 meter.
** BFEs to be changed include the listed downstream and upstream BFEs, and include BFEs located on the stream reach between the referenced locations above. Please refer to the revised Flood Insurance Rate Map located at the community map repository (see below) for exact locations of all BFEs to be changed.

Send comments to Kevin C. Long, Acting Chief, Engineering Management Branch, Mitigation Directorate, Federal Emergency Management Agency, 500 C Street, SW., Washington, DC 20472.

ADDRESSES

City of Plattsburg
Maps are available for inspection at 114 West Maple Street, Plattsburg, MO 64477.

City of Trimble
Maps are available for inspection at 201 Port Arthur Road, Trimble, MO 64492.

Unincorporated Areas of Clinton County
Maps are available for inspection at 207 North Main Street, Room 3, Plattsburg, MO 64477.

(Catalog of Federal Domestic Assistance No. 97.022, "Flood Insurance.")

Sandra K. Knight,

Deputy Assistant Administrator for Mitigation, Department of Homeland Security, Federal Emergency Management Agency.

[FR Doc. 2010–4343 Filed 3–2–10; 8:45 am]

BILLING CODE 9110–12–P

DEPARTMENT OF DEFENSE

Defense Acquisition Regulations System

48 CFR Parts 204 and 252

Defense Federal Acquisition Regulation Supplement; Safeguarding Unclassified Information (DFARS Case 2008–D028)

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

ACTION: Advance notice of proposed rulemaking (ANPR) and notice of public meeting.

SUMMARY: DoD is seeking comments from Government and industry on potential changes to the Defense Federal Acquisition Regulation Supplement (DFARS) to address requirements for the safeguarding of unclassified information. The changes would add a new subpart and associated contract clauses for the safeguarding, proper handling, and cyber intrusion reporting of unclassified DoD information within industry.

DATES: *Public Meeting:* A public meeting will be held on April 22, 2010, from 8 a.m. to 4 p.m. EST. Attendees should register for the public meeting at least 2 weeks in advance to ensure adequate room accommodations. Registrants will be given priority if room constraints require limits on attendance. Attendees wishing to make a short, issue-based 10-minute presentation on this topic should submit a copy of the presentation to the address shown below.

Special Accommodations: The public meeting is physically accessible to people with disabilities. Requests for sign language interpretation or other auxiliary aids should be directed to Mr. Julian Thrash, telephone 703–602–0310, at least 10 working days prior to the meeting date.

Submission of Comments: Comments on this ANPR should be submitted in writing to the address shown below no later than May 3, 2010.

ADDRESSES: *Public Meeting:* The public meeting will be held in the National Aeronautics and Space Administration's (NASA) James E. Webb Memorial auditorium, NASA HQ, 300 E Street SW., Washington, DC 20546. Interested parties may register by faxing the following information to DPAP(DARS) at 703–602–0350, or e-mail to *julian.thrash@osd.mil* by April 8, 2010:

(1) Company or organization name;

(2) Names of persons attending;

(3) Identity, if desiring to speak; limit to a 10-minute presentation per company or organization.

Interested parties are encouraged to arrive at least 30 minutes early. If you wish to make a presentation, please contact and submit a copy of your presentation by April 8, 2010, to Mr. Julian Thrash, OUSD (AT&L) DPAP (DARS), 3060 Defense Pentagon, Room 3B855, Washington, DC 20302–3060; Fax: 703–602–0350. Please cite "Public Meeting, DFARS Case 2008–D028" in all correspondence related to this public meeting. The submitted presentations will be the only record of the public meeting. If you intend to have your presentation considered as a public comment for the formation of a proposed rule, the presentation must be submitted separately as a written comment as instructed below.

Submission of Comments: You may submit written comments, identified by DFARS Case 2008–D028, 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 2008–D028 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), 3060 Defense Pentagon, Room 3B855, Washington, DC 20301–3060.

Hand Delivery/Courier: Defense Acquisition Regulations System, Crystal Square 4, Suite 200A, 241 18th Street, Arlington, VA 22202–3402.

Comments received generally will be posted without change to *http://www.regulations.gov,* including any personal information provided.

FOR FURTHER INFORMATION CONTACT: Mr. Julian Thrash, 703–602–0310.

SUPPLEMENTARY INFORMATION: This ANPR and notice of public meeting is a preliminary step in the rulemaking process for DFARS Case 2008–D028 that may be followed by issuance of a proposed rule in the future. The DFARS presently does not address the safeguarding of unclassified DoD information within industry, nor does it address cyber intrusion reporting for that information. The purpose of the potential DFARS changes addressed in this ANPR is to implement adequate security measures to safeguard DoD information on unclassified industry information systems from unauthorized access and disclosure, and to prescribe reporting to the Government with regard to certain cyber intrusion events that affect DoD information resident or transiting on contractor unclassified information systems. This ANPR 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. These changes to the DFARS address requirements for the safeguarding of unclassified information and may be altered as necessary to align with any future direction given in response to on-going efforts currently being led by the National Archives and Records Administration regarding Controlled Unclassified Information (CUI).

This ANPR addresses—

(1) Basic safeguarding requirements that apply to any unclassified DoD information that has not been cleared for public release in accordance with DoD Directive 5230.9, Clearance of DoD Information for Public Release; and

(2) Enhanced safeguarding requirements, including cyber incident reporting, that apply to information subject to the following:

a. Critical Program Information protection.

b. Export control under International Traffic in Arms Regulations and Export Administration Regulations.

c. Withholding from public release under DoD Directive 5400.07, DoD Freedom of Information Act Program, and DoD Regulation 5400.7–R, DoD Freedom of Information Program.

d. Controlled access and dissemination designations (e.g., For Official Use Only, Sensitive But Unclassified, Limited Distribution, Proprietary, Originator Controlled, Law Enforcement Sensitive).

e. Limitations in accordance with DoD Directive 5230.24, Distribution Statements on Technical Documents and DoD Directive 5230.25, Withholding of Unclassified Technical Data from Public Disclosure.

f. Personally Identifiable Information protection including, but not limited to, information protected pursuant to the Privacy Act and the Health Insurance Portability and Accountability Act.

The potential DFARS changes would revise the prescription for the existing clause at DFARS 252.204–7000, Disclosure of Information, and would add two new clauses for DoD information safeguarding requirements: DFARS 252.204–7XXX, Basic Safeguarding of Unclassified DoD Information Within Industry, and DFARS 252.204–7YYY, Enhanced Safeguarding and Cyber Intrusion Reporting of Unclassified DoD Information Within Industry. As the titles imply, DFARS 252.204–7XXX would require contractors to protect DoD information from unauthorized disclosure, loss, or exfiltration by employing basic information technology security measures, while DFARS 252.204–7YYY would require enhanced information technology security measures applicable to encryption of data for storage and transmission, network protection and intrusion detection, and cyber intrusion reporting. Enhanced protection measures are planned for the information specified in paragraph (2) above. A cyber intrusion reporting requirement is contemplated for enhanced protection to assess the impact of loss and to improve protection by better understanding the methods of loss; it is not required to implement the basic information safeguarding requirements at DFARS 252.204–7XXX.

DoD is interested in receiving input regarding "best practices" for protecting networks and data, experience with any of the proposed safeguards, and an evaluation of its value. In particular, DoD invites comments in the following areas:

1. What is not addressed in the draft clauses that could potentially help industry to feasibly comply with the intent of the clauses?

2. What part of the draft clauses are viewed as potentially being the most burdensome?

3. What are the potential ways to mitigate burden?

4. Are there any important information safeguarding aspects that the clauses omit that should be addressed?

5. Do the clauses as written provide clear and adequate guidance to perform safeguarding of DoD information?

6. What impact will the reporting requirement in 252.204–7YYY have on small businesses?

7. In what ways could DoD minimize the burden of the reporting requirements on respondents, including the use of automated collection techniques or other forms of information technology?

8. What are industry best practices for cyber security?

9. Should the Government establish standard information assurance criteria for all contractors as a condition of award (e.g., strong passwords, virus protection)? If so, are there existing international/national standards that should be cited or considered in building the criteria and what impediments exist to achieving this goal?

10. Would it reduce the burden without reducing effectiveness for contractors and subcontractors if the

"basic" clause were replaced with an Online Representations and Certifications Application (ORCA) certification?

11. Would it result in a more accurate cost management strategy if the "enhanced" clause were split into a safeguarding plan/program clause and a reporting clause?

12. If a contractor believes that it would have significant difficulty implementing these requirements in-house, could it out-source its information technology to a firm with specific competency in this area? If not, what are the barriers to doing so?

13. Are there any additional safeguarding or restrictions that should be implemented to protect information reported or otherwise provided to the Government under the "enhanced" clause?

List of Subjects in 48 CFR Parts 204 and 252

Government procurement.

Ynette R. Shelkin,

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. 421 and 48 CFR Chapter 1.

PART 204—ADMINISTRATIVE MATTERS

204.404–70 [Amended]

2. Section 204.404–70 is amended by removing paragraph (a) and redesignating paragraphs (b) and (c) as paragraphs (a) and (b) respectively.

3. Subpart 204.7X is added to read as follows:

Subpart 204.7X—Safeguarding and Cyber Intrusion Reporting of Unclassified DoD Information Within Industry

Sec.

Subpart 204.7X—Safeguarding and Cyber Intrusion Reporting of Unclassified DoD Information Within Industry

204.7XX0 Scope.

This subpart applies to contracts under which the contractor or a subcontractor may have unclassified DoD information resident on or transiting its unclassified information systems.

204.7XX1 Definitions.

As used in this subpart, "adequate security," "cyber," and "DoD information" are defined in the clauses at 252.204–7XXX, Basic Safeguarding of Unclassified DoD Information Within Industry, and 252.204–7YYY, Enhanced Safeguarding and Cyber Intrusion Reporting of Unclassified DoD Information Within Industry.

204.7XX2 Policy.

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

(b) Contractors must report to the Government certain cyber intrusion events that affect DoD information resident or transiting on contractor unclassified information systems. Detailed reporting criteria and requirements are set forth in the clause at 252.204–7YYY.

(c) A cyber intrusion event 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 252.204–7YYY. A cyber intrusion event must 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 intrusion events in the context of an overall assessment of the contractor's compliance with the requirements of the clause at 252.204–7YYY.

(d) DoD information requires a basic level of protection and may require an enhanced level of protection.

(1) Basic safeguarding requirements apply to any DoD information.

(2) Enhanced safeguarding requirements, including cyber incident reporting, 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) Subject to export control under International Traffic in Arms Regulations and Export Administration Regulations (see Subpart 204.73);

(iii) Designated for withholding from public release under DoD Directive 5400.07, DoD Freedom of Information Act Program, and DoD Regulation 5400.7–R, DoD Freedom of Information Program;

(iv) 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);

(v) 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

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

204.7XX3 Contract clauses.

(a) *Disclosure of information.* (1) Except as provided in paragraph (a)(2) of this section, use the clause at 252.204–7000, Disclosure of Information, in solicitations and contracts when the contractor will have access to or generate DoD information.

(2) Do not use the clause in solicitations and contracts for fundamental research unless the requiring activity has identified a validated requirement for access to or generation of DoD information to perform the fundamental research effort.

(b) *Levels of safeguarding and cyber intrusion reporting—*

(1) *Basic.* In addition to 252.204–7000, Disclosure of Information, use the clause at 252.204–7XXX, Basic Safeguarding of Unclassified DoD Information Within Industry, in solicitations and contracts when the requiring activity has identified that the contractor or a subcontractor at any tier will potentially have DoD information resident on or transiting its unclassified information systems.

(2) *Enhanced.* In addition to the clause at 252.204–7XXX, use the clause at 252.204–7YYY, Enhanced Safeguarding and Cyber Intrusion Reporting of Unclassified DoD Information Within Industry, in solicitations and contracts when the requiring activity has identified that the contractor or a subcontractor at any tier will potentially have DoD information, identified in 204.7XX2(d)(2), resident or transiting its unclassified information systems.

PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

252.204–7000 [Amended]

4. Section 252.204–7000 is amended in the introductory text by removing "204.404–70(a)" and adding in its place "204.7XX3(a)".

252.204–7003 [Amended]

5. Section 252.204–7003 is amended in the introductory text by removing "204.404–70(b)" and adding in its place "204.404–70(a)".

252.204–7005 [Amended]

6. Section 252.204–7005 is amended in the introductory text by removing "204.404–70(c)" and adding in its place "204.404–70(b)".

7. Sections 252.204–7XXX and 252.204–7YYY are added to read as follows:

252.204–7XXX Basic Safeguarding of Unclassified DoD Information Within Industry.

As prescribed in 204.7XX3(b)(1), use the following clause:

BASIC SAFEGUARDING OF UNCLASSIFIED DOD INFORMATION WITHIN INDUSTRY (XXX 2010)

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

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

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

"Data" means all non-voice information.

"DoD information" means any unclassified information that has not been cleared for public release in accordance with DoD Directive 5230.09, Clearance of DoD Information for Public Release, and that is—

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

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

"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.

"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.

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

(1) *Designation.* If the official status determination of the level of access and dissemination of the information cannot be determined, the information will be considered DoD information until the official status can be ascertained from the cognizant DoD activity.

(2) *Protecting DoD information on public computers or Web sites:* Do not process DoD 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. DoD information shall not be posted on Web sites that are publicly available or have access limited only by domain/IP 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 Web site itself or the application it hosts).

(3) *Transmitting electronic information.* Transmit e-mail, 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.

(4) *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.

(5) *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.

(6) *Sanitization.* Sanitize media in accordance with National Institute of Standards and Technology (NIST) 800–88, Guidelines for Media Sanitization, at *http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf,* before external release or disposal.

(7) *Intrusion protection.* Provide protection against computer intrusions and data exfiltration, minimally including the following:

(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.

(8) Limitations. Transfer DoD 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, if the subcontractor will have access to or generate DoD information.

(End of clause)

252.204–7YYY Enhanced Safeguarding and Cyber Intrusion Reporting of Unclassified DoD Information Within Industry.

As prescribed in 204.7XX3(b)(2), use the following clause:

ENHANCED SAFEGUARDING AND CYBER INTRUSION REPORTING OF UNCLASSIFIED DOD INFORMATION WITHIN INDUSTRY (XXX 2010)

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

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

"Advanced persistent threat" means an extremely proficient, patient, determined, and capable adversary, including such adversaries working together.

"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).

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

"Critical Program Information (CPI)" (formerly Essential Program Information, Technologies and/or Systems) 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 all non-voice information.

"DoD information" means any unclassified 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.

"Encryption" means the protection of data in electronic form, in storage or in transit, using an encryption technology that has been approved the National Institute of Standards and Technology or the National Security Agency.

"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.

"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.

"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) *Enhanced safeguarding requirements and procedures*—

(1) *Adequate security.* The Contractor shall—

(i) Provide adequate security to safeguard DoD information on its unclassified information systems from unauthorized access and disclosure;

(ii) Safeguard all DoD information in accordance with the basic requirements set forth in the clause of this contract entitled "Basic Safeguarding of Unclassified DoD Information Within Industry" (DFARS 252.204–7XXX); and

(iii) Safeguard DoD information described in paragraph (b)(2) of this clause in accordance with the requirements in paragraph (b)(3) of this clause.

(2) *DoD information requiring enhanced safeguarding.* Enhanced safeguarding requirements, including cyber incident reporting, 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) Subject to export controls under International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR);

(iii) Designated for withholding from public release under DoD Directive 5400.07, DoD Freedom of Information Act Program, and DoD Regulation 5400.7–R, DoD Freedom of Information Program;

(iv) 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);

(v) 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

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

(3) *Enhanced safeguarding requirements.* The Contractor shall apply the following enhanced safeguarding requirements for DoD information:

(i) *Encryption/Storage.* Encrypt using the Security Controls for Federal Information Systems and Organizations at (*http://csrc.nist.gov/publications/PubsSPs.html*) for both organizational wireless connections, and when traveling use encrypted wireless connections where available. If encrypted wireless is not available, encrypt application files (*e.g.,* spreadsheet and word processing files) using at least application-provided password protection level encryption. Encrypt all information identified in paragraph (b)(2) of this clause when it is stored on mobile computing devices such as laptops and personal digital assistants, or removable storage media such as thumb drives and compact disks, using the best level of encryption technology available, given facilities, conditions, and environment.

(ii) Network intrusion protection. Provide adequate protection against computer network intrusions and data exfiltration, as follows:

(A) Current and regularly updated malware protection services, *e.g.,* anti-virus, anti-spyware.

(B) Monitoring and control of both inbound and outbound network traffic as appropriate (*e.g.,* at the external boundary, sub-networks, individual hosts) to include blocking unauthorized ingress, egress, and exfiltration through technologies such as firewalls and router policies, intrusion prevention or detection services, or host-based security services.

(C) Prompt application of security-relevant software patches, service-packs, and hot fixes.

(iii) The Contractor shall implement information security controls in its project, enterprise, or company-wide unclassified information security program. The information security program shall address the security controls described in the NIST Special Publication 800–53 (Current Version), Recommended Security Controls for Federal Information Systems and Organizations (*http://csrc.nist.gov/publications/PubsSPs.html*), and should be tailored in scope and depth appropriate to the effort and the specific unclassified DoD information.

(4) *Other requirements.* This clause does not relieve the Contractor of the requirements specified by other Federal and DoD safeguarding requirements for specified categories of information (*e.g.,* CPI, PII, For Official Use Only, Privacy Act, ITAR, EAR, and HIPAA), as specified by applicable regulations or directives.

(c) *Cyber intrusion reporting*—

(1) *Reporting requirement.* The Contractor shall report to the Defense Cyber Crime Center's (DC3) DoD–DIB Collaborative Information Sharing Environment (DCISE) (URL to be determined) within 72 hours of discovery of any cyber intrusion events that affect DoD information resident on or transiting the Contractor's unclassified information systems.

(2) *Reportable events.* Reportable cyber intrusion events include the following:

(i) A cyber intrusion event appearing to be an advanced persistent threat.

(ii) A cyber intrusion event involving data exfiltration or manipulation or other loss of any DoD information resident on or transiting its, or its subcontractors', unclassified information systems.

(iii) Intrusion activities not included in paragraph (c)(2)(i) or (ii) of this clause that allow illegitimate access to an unclassified information system on which DoD information is resident or transiting.

(3) *Other reporting requirements.* This reporting in no way abrogates the Contractor's responsibility for additional safeguarding and cyber intrusion 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.,* CPI, PII, Privacy Act, ITAR and EAR, and HIPAA).

(4) *Contents of the incident report.* The incident report shall include, at a minimum, the following information:

(i) Applicable dates (date of compromise and/or date of discovery).

(ii) Threat methodology (all known resources used such a Internet Protocol (IP) addresses, domain names, software tools, etc.).

(iii) An account of what actions the adversary may have taken on the victim system/network, and what information may have been accessed.

(iv) A description of the roles and function of the threat-accessed systems.

(v) Potential impact on DoD programs or an initial list of impacted DoD programs.

(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 unclassified information systems accessed by a threat to identify specific DoD information files associated with DoD contracts or systems, military applications, and militarily critical technology for evidence of intrusion.

(ii) Preserve and protect images of the known affected systems until DC3 has

received the image and completes its analysis.

(iii) Cooperate with DC3 to ascertain intruder methodology and identify systems compromised as a result of the intrusion. The DCISE Web site will provide detailed guidelines and processes as needed and appropriate.

(iv) As required by the Government and permitted by law, share files on compromised systems that pertain to unclassified DoD information.

(6) *Damage assessment activities.* The DoD Damage Assessment Management Office (DAMO) will conduct an initial damage assessment and notify the Contractor whether a follow-up compromise assessment report is required. If required, the follow-up report shall include at a minimum the following information:

(i) An index of DoD information contained on the affected system.

(ii) An initial list of DoD programs impacted by the compromise.

(iii) The type of DoD information compromised (*e.g.,* CPI, PII, Privacy Act, ITAR, EAR, and HIPAA) and a brief description of the accessed information.

(iv) The Contractor's points of contact to coordinate future damage assessment activities.

(v) The threat methodology.

(vi) Amount of DoD information including files/data bytes exfiltrated or accessed.

(vii) Inventory of DoD IT equipment accessed or from which DoD information has been exfiltrated.

(d) *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.,* CPI, PII, FOIA, Trade Secrets Act, Privacy Act, ITAR, EAR, and HIPAA).

(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 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 the DCISE 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 best practices) 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.

(e) 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.

(f) *Subcontracts.* The Contractor shall include the substance of this clause, including this paragraph (f), in all subcontracts under this contract, if the subcontractor will have access to or generate DoD information. 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 DCISE as required by paragraph (c) of this clause.

(End of clause)

[FR Doc. 2010–4173 Filed 3–2–10; 8:45 am]

BILLING CODE 5001–08–P

DEPARTMENT OF TRANSPORTATION

Office of the Secretary

49 CFR Part 71

[OST Docket No. OST–2010–0046]

Standard Time Zone Boundary in the State of North Dakota: Proposed Change for Mercer County, North Dakota, From Mountain to Central Time Zone

AGENCY: Office of the Secretary, Department of Transportation (DOT).

ACTION: Notice of Proposed Rulemaking (NPRM).

SUMMARY: The Chairman of the Board of County Commissioners for Mercer County, North Dakota, petitioned the U.S. Department of Transportation to move Mercer County from the mountain to the central standard time zone. The Department believes that the petition makes a prima facie case for the proposed time zone change, and we are using this notice to solicit public comment on the proposal.

DATES: Public comments to the docket should be submitted by June 14, 2010. Late-filed comments will be considered to the extent practicable. The Department has scheduled a public hearing on this issue from 7–10 p.m. (Mountain Daylight Time) on Friday, May 14, 2010, in the "Large Room" of the City Hall, 146 East Main Street, Hazen, North Dakota.

ADDRESSES: You may submit comments (identified by the agency name and DOT Docket ID Number OST–2010–0046) by any of the following methods:

- *Federal eRulemaking Portal:* Go to *http://www.regulations.gov* and follow the online instructions for submitting comments.
- *Mail:* Docket Management Facility: U.S. Department of Transportation, 1200 New Jersey Avenue, SE., West Building Ground Floor, Room W12–140, Washington, DC 20590–0001.
- *Hand Delivery or Courier:* West Building Ground Floor, Room W12–140, 1200 New Jersey Avenue, SE., between 9 a.m. and 5 p.m. ET, Monday through Friday, except Federal holidays.
- *Fax:* 202–493–2251.

Instructions: You must include the agency name (Office of the Secretary, DOT) and Docket number (OST–2010-) for this notice at the beginning of your comments. You should submit two copies of your comments if you submit them by mail or courier. Note that all comments received will be posted without change to *http://www.regulations.gov* including any personal information provided and will be available to internet users. You may review DOT's complete Privacy Act Statement in the **Federal Register** published on April 11, 2000 (65 FR 19477) or you may visit *http://DocketsInfo.dot.gov.*

Docket: For internet access to the docket to read background documents and comments received, go to *http://www.regulations.gov.* Background documents and comments received may also be viewed at the U.S. Department of Transportation, 1200 New Jersey Avenue, SE, Docket Operations, M–30, West Building Ground Floor, Room W12–140, Washington, DC 20590, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

FOR FURTHER INFORMATION CONTACT: Robert C. Ashby, Deputy Assistant General Counsel for Regulation and Enforcement, U.S. Department of Transportation, Room W94–302, 1200 New Jersey Avenue, SE., Washington, DC 20590, (202) 366–9310, *bob.ashby@dot.gov.*

SUPPLEMENTARY INFORMATION: For more than a century, time zone boundaries in North Dakota have had an interesting and varied history. Beginning in 1883, mountain time was observed in the southwest portion of the state and a few locations in the northwest, with central time being used elsewhere. In 1929, the Interstate Commerce Commission (ICC), which then had jurisdiction over time zone boundaries, extended central time to cover all but a cluster of counties in