VENABLE LLP

government contracts alert

www.Venable.com
July 2011

Please contact any of the attorneys in our Government Contracts Group if you have any questions regarding this alert.

Authors

Robert A. Burton
rburton@Venable.com
202.344.4776

Dismas Locaria
dlocaria@Venable.com
202.344.8013

Proposed DFARS Rule Would Impose New Protection and Reporting Requirements on Defense Contractors

On June 29, 2011, the Department of Defense (DoD) proposed a rule to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to add a new subpart and contract clauses to require the safeguarding of unclassified DoD information and mandate the reporting of "cyber incidents." 76 Fed. Reg. 38089 (June 29, 2011). This rule addresses the safeguarding requirements specified in Executive Order 13556 (E.O. 13556 or the Order), Controlled Unclassified Information, dated November 4, 2011. The proposed rules have significant implications for DoD contractors possessing certain types of unclassified information in terms of safeguarding such information and reporting certain incidents as outlined below.

Executive Order 13556: Before E.O. 13556, there was no common framework for describing how: 1) an unclassified document should be marked; 2) under what circumstances a document should no longer be considered sensitive but unclassified (SBU); and 3) what procedures governed the safeguarding and dissemination of SBU information. E.O. 13556 established a program for managing all unclassified information in the Executive Branch that requires safeguarding or dissemination controls, pursuant to, and consistent with, applicable law, regulations, and government-wide policies. The Order states that such information, described as Controlled Unclassified Information or "CUI", will now be regulated by an "open and uniform program." This program is being administered by the National Archives and Records Administration (NARA).

The Order established a relatively narrow timeframe for implementation. Specifically, within 180 days from the date of the Order, each agency must submit a catalogue of proposed categories and subcategories of CUI. Within the same 180-day time period, NARA, in consultation with the affected agencies, must issue initial directives for the implementation of the Order. Then, within 180 days from the issuance of the initial directives by NARA, each agency that handles CUI must provide the NARA with a proposed plan for compliance with the requirements of the Order, including interim target dates. Within one year from the date of the Order, NARA must establish and maintain a public CUI registry reflecting the authorized CUI categories and subcategories, associated markings, and applicable safeguarding, dissemination, and decontrol procedures.

The Proposed DFARS Rule: In response to E.O. 13556, the Department of Defense issued a proposed rule that created a two-tiered program: basic and enhanced safeguarding. The objective of this rule is for DoD to avoid the disclosure 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 program applies to the following types of information:

- information designated as critical program information in accordance with DoD Instruction 5200.39, Critical Program Information (CPI) Protection;
- information designated as critical information in accordance with DoD Directive 5205.02, DoD Operations Security;
- information subject to export controls under International Traffic in Arms Regulations and Export Administration Regulations;
- information exempt from mandatory public disclosure under DoD Directive 5400.07, DoD Freedom of Information Act (FOIA) Program;
- information 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);
- information that is 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
- information 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.

In implementing this program, the proposed rule revises one DFARS clause and creates two new clauses. DFARS 252.204-7000, Disclosure of Information is modified to add a definition of ''DoD information,'' and ''nonpublic information.'' The two new clauses are:

1. 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.

2. 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.

Under the reporting requirements of the enhanced safeguarding clause, contractors shall be required to report to DoD within 72 hours of the discovery of a "cyber incident." A reportable "cyber incident" includes the following:

- 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; or
- certain incidents that allow unauthorized access to an unclassified information system on which DoD information is resident or transiting.

Impact to Contractors: For the basic protection, DoD believes the resultant cost impact will 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. DoD further believes 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.

With respect to information requiring enhanced protections, 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 also 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 small and mid-size businesses have less sophisticated programs and will incur costs in meeting the additional requirements.

Practitioner's Tips: While these DFARS clauses are proposed rules at this time, contractors should be mindful that cyber-related information safeguards, even for unclassified information, will become more frequent as agencies begin implementing the program set forth in E.O. 13556. As a result, contractors should:

- assess their current information technology safeguards;
- determine whether these are adequate in the industry and adaptable to what may be required in the public and private sphere in the future;
- understand the likely requirements of government rules and regulations, including "enhanced" safeguarding and reporting requirements; and
- stay abreast of changes in the government's regulatory landscape, and participate in the discussion and interpretation of this landscape.

Venable has a diverse cadre of attorneys and professionals that assist clients in each of these areas. For more information or assistance, please contact the authors of this article or any member of the Government Contracts Group.
