VENABLE® LLP

Government Contracts Update

August 28, 2012

FISMA Extension: New Information Safeguarding Requirements Proposed for Government Contractors

AUTHORS

Paul A. Debolt

Keir X. Bancroft

RELATED PRACTICES

Government Contracts

RELATED INDUSTRIES

Government Contractors

ARCHIVES

2012 2008 2004
2011 2007 2003
2010 2006 2002
2009 2005

Government contractors should take note of a newly proposed FAR rule that requires basic safeguards for government contractor information systems. Under the proposed rule, government contractor information systems that contain or process information provided by or generated for the government (other than public information) will need to have the following safeguards that:

- **Restrict Information:** Restrict information on public computers or Web sites without access control;
- **Protect Transmissions:** Protect electronic information transmissions, including e-mail, text messages, blogs, and similar communications;
- **Protect Voice and Fax Transmissions:** Limit voice and fax transmissions to authorized recipients;
- **Apply Physical and Electronic Security:** Provide physical and electronic barriers to information provided by or generated for the government;
- **Sanitize Media:** Clear information from media used to process information;
- **Protect Against Intrusion:** Apply protection against computer intrusions and data compromise by regularly updating anti-virus software and anti-spyware and promptly applying patches, service packs, and hot fixes; and
- **Limit Information Transfers:** Limit transfers of information only to subcontractors that require the information for contract performance, and have the same level of security as prescribed by the government.

These requirements will be widely applicable. They are prescribed under a new FAR clause, applicable pursuant to a newly proposed FAR subpart 4.17, Basic Safeguarding of Contractor Information Systems. The subpart will apply to commercial items and commercial off-the-shelf (COTS) items when information provided by or generated for the government (other than public information) will reside on or transit through a contractor's information system. A contracting officer will be allowed to apply the safeguarding requirements even at levels under the simplified acquisition threshold when inclusion is determined appropriate.

This proposed rule does not apply to public information, which an agency "discloses, disseminates, or makes available to the public." Instead, it applies to information defined by the Committee on National Security Systems Instruction 4009 as "any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual."

The proposed rule extends applicability of the Federal Information Security Management Act (FISMA), which generally requires risk-based protection against unauthorized access, use, disclosure, disruption, modification, and destruction of federal agency information. The rule prescribes basic security for information and information systems that support the operations and assets of a federal agency, including those managed by contractors. The proposed FAR subpart expressly extends those responsibilities to contractors and subcontractors as well.

In analyzing the economic impact of the rule, DoD, NASA and GSA took the position that the proposed rule applies to all federal contractors and subcontractors, regardless of whether the contractor is a large or small business. The cost of the rule was deemed insignificant, since the first-level protective measures (including virus protection and software patches) are typically employed as part of the regular course of doing business. It was also concluded that the "prudent business practices designed to protect an [IT] system are typically a common part of everyday operations."

Public comments on the Proposed Rule are due October 23, 2012. More information is available at **www.regulations.gov**, under FAR Case 2011-020. For more information on these or other government contractor information security requirements, please contact **Paul Debolt** at **padebolt@Venable.com**, **Keir Bancroft** at **kxbancroft@Venable.com**, or any of the other attorneys

in Venable's **Government Contracts Practice Group**.