

Government Contracts Update

January 2012

GSA Requires IT Contractors to Create and Implement IT Security Plans: This May Only Be the Beginning

AUTHORS

Rebecca E. Pearson
Andrew E. Bigart
Dismas Locaria

RELATED PRACTICES

Government Contracts

RELATED INDUSTRIES

Government Contractors

ARCHIVES

2012 2008 2004
2011 2007 2003
2010 2006 2002
2009 2005

On January 6, 2012, the General Services Administration ("GSA") issued a final rule (77 Fed. Reg. 749 (Jan. 6, 2012)) requiring all prime- and sub-contractors providing the GSA with information technology ("IT") supplies, services, or systems to submit an IT security plan outlining compliance with federal cybersecurity regulations. The GSA acknowledges that "[t]his final rule may have a significant economic impact on a substantial number of small entities." The new rule signals what may become standard for all government contractors, and perhaps all commercial entities, in the years to come, as the U.S. government (and private industry) react to the rapidly developing cybersecurity landscape.

OIG Recommends Strengthening Security Requirements for IT Supplies, Services and Systems

The final rule stems from an audit conducted by the GSA Office of the Inspector General ("OIG") that determined that the GSA's information and IT systems failed to meet the requirements of the Federal Information Security Management Act of 2002 ("FISMA"). Following the audit, the OIG made recommendations to strengthen the security requirements in contracts and orders for IT supplies, services and systems. The GSA agreed with the OIG's recommendations and developed and published an interim rule, with a request for comments (76 Fed. Reg. 34,886 (June 15, 2011)), requiring GSA IT contractors to submit an IT security plan outlining compliance with federal cybersecurity regulations. The final rule implements the interim rule with only minor changes.

Contractors Must Develop IT Security Plans and Monitoring Procedures

The interim rule provides that contracting officers shall insert GSAR 552.239-70, Information Technology Security Plan and Security Authorization, in all solicitations for IT supplies, services or systems in which the contractor will have physical or electronic access to government information that directly supports the GSA's mission. GSAR 552.239-70 provides that "[a]ll offers/bids submitted in response to this solicitation must address the approach for completing the security plan and certification and security authorization requirements as required by the clause 552.239-71, Security Requirements for Unclassified Information Technology Resources."

GSAR 552.239-71 provides that:

"The Contractor shall be responsible for information technology (IT) security, based on General Services Administration (GSA) risk assessments, for all systems connected to a GSA network or operated by the Contractor for GSA, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor has physical or electronic access to GSA's information that directly supports the mission of GSA, as indicated by GSA."

76 Fed. Reg. 34,886, 34,889 (Jun. 15, 2011). To ensure IT security, GSAR 552.239-71 further requires contractors to develop, provide, implement and maintain an IT security plan. Specifically:

- The plan must describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed or used under the contract;
- The plan must describe those parts of the contract to which GSAR 552.239-71 applies;
- A contractor's IT security plan must comply with applicable federal laws that include, but are not limited to, 40 U.S.C. § 11331, FISMA, and the E-Government Act of 2002; and
- The plan must satisfy IT security requirements in accordance with federal and GSA policies and procedures.

The clause also requires that the CIO IT Security Procedural Guide 09-48, Security Language for

Information Technology Acquisition Efforts, issued by the GSA Chief Information Officer, be incorporated by reference in all solicitations, contracts and task orders where an information system is contractor-owned and operated on behalf of the federal government.

Finally, the plan must include a continuous monitoring strategy that includes:

- A configuration management process for the information system and its constituent components;
- A determination of the security impact of changes to the information system and environment of operation;
- Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
- Reporting on the security state of the information system to appropriate GSA officials; and
- Implementation of continuous monitoring by all GSA general support systems and applications in accordance with the rule and National Institute of Standards and Technology SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

In the final rule, GSA has adopted the interim rule with minor changes. Contractors must submit their IT security plans within thirty calendar days after contract award. The plan submitted by contractors must be consistent with, and specify in greater detail, the approach contained in the contractors' bid proposals. In particular, the final rule requires contractors to grant GSA inspectors access to facilities, operations, documents, databases and all else needed to determine that such contractor is in compliance with federal cybersecurity standards.

The rule applies to contracts and orders awarded after January 6, 2012 that include IT supplies, services and systems with security requirements.

Rule Demonstrates Increased Emphasis by Federal Government on Protecting Against Cybersecurity Attacks

Notwithstanding the fact that the GSA openly acknowledged in 2011 that this rule "may have a significant economic impact on a substantial number of small entities" (76 Fed. Reg. at 34,887), the GSA adopted the interim rule with only minor changes. This represents the increasing significance and concern the federal government is placing on the security of its IT systems from cyberattack.

Contractors should not only be mindful of the GSA's new requirements, but expect such requirements to permeate throughout federal contracting. Accordingly, contractors may want to consider the company-wide application of its security plans when designing and developing any plan.

Finally, contractors should monitor further developments in generally applicable cybersecurity legislation and regulation as Congress and agencies have become increasingly active in addressing cybersecurity concerns. For instance;

- Congress has been **constantly considering cyber legislation**.
- On May 12, 2011, President Obama unveiled an **International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World**, which set forth the Administration's long-term strategies for managing global cybersecurity.
- The Securities and Exchange Commission **issued cybersecurity guidelines** for publicly traded companies.

For more information, please contact any of the attorneys in Venable's **Government Contracts Practice Group**.