AN ALERT FROM THE BDO GOVERNMENT CONTRACTING PRACTICE

BDO KNOWS:
GOVERNMENT CONTRACTING

CYBERSECURITY ALERT:
Final FAR Cyber Rule on Safeguarding of Contractor Information

In May, the Department of Defense (DOD), General Service Administration (GSA) and the National Aeronautics and Space Administration (NASA) issued a long-awaited Final Rule amending the Federal Acquisition Regulations (FAR) with a new subpart and contract clause for the basic safeguarding of contractor information systems that contain or process information provided by or generated for the government.

This rule comes almost four years after a proposed rule on the subject was first issued in August 2012.

Nearly all federal contracts will require contractors to implement a set of cyber hygiene measures aimed at ensuring the "basic safeguarding" of any of their systems that possess, store or transmit a newly and broadly defined category of "federal contract information." Information systems that are owned or operated by federal contractors and contain or process federal contract information will need to be compliant with all of the rule's required security controls.

The new rule is effective as of June 15, 2016.

DETAILS

"Federal contract information" is broadly defined as "information, not intended for public release, that is provided by or generated for the government under a contract to develop or deliver a product or service to the government, but not including information provided by the government to the public (such as on public websites) or simple transactional information, such as necessary to process payments."

The amendments to FAR require that the new clause be included in contracts for "all acquisitions, including acquisitions of commercial items other than commercially available off-the-shelf items, when a contractor's information system may contain federal contract information."

The clause will also cover most subcontracts. It requires contractors to flow down the clause (including the flowdown itself) in subcontracts (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items) in which the subcontractor may have federal contract information residing in or transmitted through its information system.

The contract clause lists 15 security controls that federal contractors will be required

Read more ▶

BDO KNOWS GOVERNMENT CONTRACTING

For more information on how BDO professionals can help strengthen your cybersecurity infrastructure and protect your systems, please contact:

SHAHRYAR SHAGHAGHI
Technology Advisory Services National Leader and Head of International BDO Cybersecurity
212-885-8453 / sshaghaghi@bdo.com

DEENA COFFMAN
BDO Consulting Managing Director
212-798-4037 / dcoffman@bdo.com

BOB CRAIG
Managing Director, Government Contract Advisory Services
703-770-1095 / rcraig@bdo.com

to implement to satisfy a "basic" level of safeguarding of federal contract information. The required controls include:

- Limit information system access to authorized users, processes acting on behalf of authorized users, or devices.
- Limit information system access to only permitted transactions and functions of authorized users.
- Verify identities of users, processes and devices as a prerequisite to access of organizational information systems.
- Limit physical access to organizational information systems, equipment and operating environments to authorized individuals.
- Monitor, control and protect organizational communications at the external and key internal boundaries of the information systems.
- Identify, report and repair system and information flaws in a timely manner.
- Perform regular scans of the information systems and real-time scans of files from external sources as files are downloaded, opened and used.

The Final Rule does not absolve contractors from other safeguarding requirements specified by government agencies, and is "just one step in a series of coordinated regulatory actions being taken or planned to strengthen protections of information systems." Contractors entrusted with safeguarding sensitive information will, in most cases, be required to implement more stringent controls. Additional regulations, including cybersecurity measures addressing the use and dissemination of Controlled Unclassified Information (CUI), are pending.

BDO INSIGHTS

The rule establishes *minimum* cybersecurity standards for contractors' information systems. From a liability perspective, as long as the required basic controls are in place, failure of the controls to protect federal contract information will not constitute a breach of contract.

However, from a competitive perspective, contractors should consider that these basic measures are viewed by the government as the *lowest acceptable level of cybersecurity*. To be competitive, contractors must *at least* meet—and ideally exceed—these standards.

Contractors may want to look to the recent amendments to the Defense Federal Acquisition Regulation Supplement (DFARS), a more rigorous set of standards for contractors handling sensitive DOD information. The new DFARS procedures direct contractors to implement the National Institute of Standards and Technology (NIST) framework for protecting sensitive government information. The NIST framework, finalized last June, aims to provide a consistent approach across agencies and is considered the "gold standard" of cyber preparedness.

Notably excluded from the FAR amendment for all federal contractors is the requirement for annual reporting of the overall effectiveness of an organization's information security program and any remedial actions that took place over the course of the year. The FAR Final Rule also does not provide explicit cyber-incident reporting instructions—though it does state incidents must be reported in a "timely manner"—or permit the relevant government agency to conduct its own data analysis.

With more cyber regulations coming down the pike, contractors would be wise to go beyond the basic safeguarding requirements laid out in the FAR Final Rule and proactively adopt the recommendations from the NIST framework.

BDO assists government contractors in performing security risk assessments, testing controls and conducting security monitoring, in addition to implementing cybersecurity risk management programs, strategy and governance in line with federal requirements and best practices.

People who know Government Contracting, know BDO.