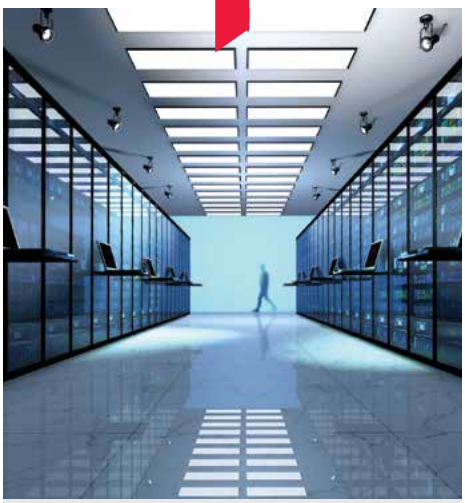
AN ALERT FROM THE BDO GOVERNMENT CONTRACTING PRACTICE

BDO KNOWS:
GOVERNMENT CONTRACTING



6 CYBERSECURITY QUESTIONS GOVERNMENT CONTRACTORS SHOULD ADDRESS

By Gregory Garrett and Karen Schuler

With cyberattackers growing increasingly sophisticated in their methods and the number of data breaches on the rise, it's no wonder that cybersecurity is top of mind for both the public and private sectors. In fact, the numerous attacks in recent years have been serious and costly enough to prompt action at the federal level.

On May 1, the Trump administration released an executive order mandating that all U.S. federal government agencies plan, develop and submit formal cybersecurity risk management plans to help safeguard their sensitive information and controlled unclassified information (CUI). This new cybersecurity EO is designed to promote cyber risk mitigation across the entire government by holding each agency head personally responsible for network protection and requiring all agencies to modernize their information technology systems. In addition to the cybersecurity EO, each agency is also expected to use the National Institute of Standards and Technology's Cybersecurity Framework to enhance its controls and management of CUI.

The government is also requiring government contractors to be held accountable to similar cybersecurity standards, dictated by the NIST Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations." NIST SP 800-171 provides 109 individual controls categorized under 14 families of information security requirements designed to help companies control the security of their CUI. This set of cybersecurity requirements is soon to be implemented across government contractors via a new final rule to the Federal Acquisition Regulation, which is an expansion of the current U.S. Department of Defense's Defense Federal Acquisition Regulation Supplement implemented in June 2016.

With these additional regulations on the horizon, it's not surprising that many government contractors feel overwhelmed; after all, they must now comply with several new requirements on top of the numerous industry-specific and international cyber

HOW DO I GET MORE INFORMATION?

CHRISTOPHER CARSON
National Government Contracting Practice Lead, Audit Partner
703-770-6324 / ccarson@bdo.com

ERIC SOBOTA
National Leader, Government Contracts and Grants Advisory Services
703-770-6395 / esobota@bdo.com

JOE BURKE
Partner, Transaction Advisory Services
703-770-6323 / jburke@bdo.com

STEPHEN RITCHEY
Audit Partner
703-770-6346 / sritchey@bdo.com

JEFF SCHRAGG
Tax Partner
703-770-6313 / jschragg@bdo.com

DEREK SHAW
Director
703-336-1501 / dshaw@bdo.com

ANDREA WILSON
Managing Director, Grants Advisory Services
703-752-2784 / aewilson@bdo.com

Read more ▶

standards, such as ISO 27001, already in place. As a result, many government contractors are experiencing numerous pain points related to the implementation of cybersecurity information governance, risk management and compliance.

Based on our discussions with more than 100 government contractors in recent months, we have outlined the top six cybersecurity questions they should address below.

1. How can government contractors accurately and cost effectively assess their cybersecurity compliance to NIST SP 800-171?

First, it is important to understand that NIST SP 800-171 is a set of guidelines established to help companies protect their CUI and DOD covered defense information (CDI) in nonfederal systems and organizations. CUI is a result of the Obama administration Executive Order 13556, issued in November 2010. The CUI system aims to standardize and simplify how the government handles unclassified information that requires safeguarding. There are 22 approved CUI categories of information, covering everything from agriculture, transportation and energy to defense technical drawings and product specifications provided by federal government agencies to government contractors.

Second, according to NIST, there are two classifications of security requirements: basic and derived. The basic security requirements are obtained from the Federal Information Processing Standard 200, which provides high-level fundamental security requirements for federal information and information systems. The derived security requirements, which supplement the basic security requirements, are taken from the detailed security controls contained in NIST Special Publication 800-53.

Third, for a government contractor to ensure it receives an accurate and cost-effective assessment of its cybersecurity capabilities in comparison to the NIST SP 800-171 guidelines, it should competitively evaluate and select an independent professional services company with the ability to perform a high-quality and timely cyberrisk and gap assessment.

Currently, it appears that many government contractors do view the NIST 800-171 guidelines as a mandatory rule that requires full and strict compliance. It is expected that the new DFARS 252.204-7012 cybersecurity and information security management system will be treated in the same manner as the six current major contractor business systems: accounting, cost estimating, material management and accounting system, government property management and earned value management system.

2. What actions do U.S. government contracting officers plan to take if government contractors fail to comply with the DFARS 252.204-7012 (NIST SP 800-171 compliance requirement) after the Dec. 31, 2017, deadline?

So far, government contractors have been advised via updates from the DOD chief information officer that the Defense Contract Management Agency may request a copy of their system security plan (SSP) for purposes of evaluation for compliance with the NIST SP 800-171 requirements and that the Defense Contract Audit Agency may audit their related information security management systems' cost.

Concerns to consider:

- Currently, neither the DCAA nor the DCMA has the necessary cybersecurity expertise to assess the contractor's compliance with the standard. Without certified information system security professionals, certified information technology auditors or the like, they cannot accurately evaluate government contractors' SSPs to fairly assess their compliance with NIST SP 800-171.
- If the federal government decides to outsource the SSP evaluation to assess compliance with NIST SP 800-171, it is imperative to ensure that the selected companies are free of organizational conflicts of interest and personal conflicts of interest.
- If a government contractor is noncompliant with all or part of NIST SP 800-171, then the government contracting officer will have to decide on a number of actions. He or she can:
  - Withhold contractor payments up to 20 percent;
  - Issue a stop work order;
  - Issue a suspension of work; or
  - Terminate the contract for default.

3. How should government contractors pay for this additional cybersecurity compliance expense?

The DCAA has not yet provided specific guidance on how the new cybersecurity compliance-related expenses will be audited. Nevertheless, these costs will likely be audited in a similar manner to the six existing DFARS contractor business systems. Compliance-related business expenses may be categorized as a direct or indirect cost, depending on the contract requirements and the contractor's accounting system. Often, these DFARS contractor business system requirements are considered indirect costs. Thus, if these cybersecurity management system-related compliance costs are charged as indirect costs, properly allocated and considered fair and reasonable in both nature and amount, they should be deemed as allowable costs.

Read more ▶

4. Do I have to purchase cybersecurity liability insurance?

Currently, the FAR and DFARS do not require government contractors to purchase cybersecurity liability insurance.

Concerns to consider:

- If a government contractor does purchase cyber liability insurance, will the cost of the insurance be considered as an allowable cost on a government contract?
- How much cyber liability insurance will be considered sufficient by the federal government and deemed an allowable cost?
- If a government contractor experiences a cyberattack that results in a network breach and its insurance provider denies some or all of the security-related breach remediation costs, will costs, if fair and reasonable in nature and amount, be deemed an allowable cost on a government contract?

5. Will prime government contractors be held contractually responsible and financially liable for cyber-related damages caused by their subcontractors and/or third-party partners' failure to comply with NIST SP 800-171?

The FAR states that prime contractors are responsible for the selection, administration and performance of their subcontractors.

Concerns to consider:

- The contract between prime contractor and a subcontractor is a commercial contract. Subcontractors have no privity of contract with the government. Often, prime contractors do not communicate all the appropriate government requirements to their subcontractors.
- Prime contractors often attempt to contractually transfer all responsibilities and financial liabilities to their subcontractors.

6. How can government contractors staff and retain high-quality cybersecurity talent to meet the increasing number of government information security compliance standards when considering the highly competitive marketplace and global shortage of cybersecurity professionals today?

The recruiting, staffing, training and retention of cybersecurity talent is a significant challenge for nearly every organization. The global shortage of experienced cybersecurity professionals is expected to increase over the next three to five years. Thus, the need to create the right balance of cybersecurity employees, tools and managed outsourced services becomes vital to all public and private organizations, especially for small to midsize companies.

SUMMARY

As government contractors are required to comply with new U.S. regulatory requirements every year, they are also experiencing a rise in compliance-related costs. Many government contractors will sometimes decide to defer them to see if the government will enforce the new guidelines. If they are enforced, contractors will often wait to see how much the penalties are — and if they are greater than the cost of compliance — to decide whether they should bear the additional expenses.

Government contractors often find themselves facing a dilemma: They must figure out the best way they can properly safeguard their CUI and ensure compliance with the NIST SP 800-171 guidelines, while continuing to remain competitive in the federal marketplace and achieve a fair and reasonable return on investment.

*Originally **published** on Law360*

Gregory A. Garrett is head of international cybersecurity at BDO USA LLP in Washington, D.C. Previously, he was head of cybersecurity for the UIC Corporation and Blue Canopy Group LLC, managing director for Navigant Consulting Government Services, and chief compliance officer, chief information security officer and vice president and general manager of program management for Lucent Technologies Inc.

Karen Schuler is a partner in BDO's Washington office and head of the information governance practice. She is a former member of the U.S. Securities and Exchange Commission's forensic team.

People who know Government Contracting, know BDO.

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 550 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 67,700 people working out of 1,400 offices across 158 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your firm's individual needs.