wiley

NEWSLETTER

Government Contractor Cybersecurity Requirements and Guidance Continue to Evolve

February 2016

Government Contracts Issue Update

Over the last six months, cybersecurity guidance and requirements for government contractors continued to evolve, with significant developments for U.S. Department of Defense (DOD) contractors and the announcement of imminent new rules for civilian agency contractors. These developments will continue to have a profound impact on compliance efforts contractors are undertaking to secure government information that resides on contractor information systems. This article provides an overview and update on these developments, first for defense contractors and then for their civilian counterparts.

DOD Rules for Safeguarding Information Continue to Evolve

Following the November 2013 final rule implementing DOD's requirements for Safeguarding Unclassified Controlled Technical Information (UCTI), which adopted select standards from NIST Standard Publication (SP) 800-53 as the baseline for securing UCTI residing on contractor systems, DOD issued an interim rule on August 26, 2015, that made sweeping changes to the scope of the rule and the baseline requirements. *See* 80 Fed. Reg. 51739. Among the most significant changes:

DOD revised its baseline security standards from NIST SP 800-53 to a new NIST standard, SP 800-171, that was prepared specifically for government contractor systems and finalized earlier in the summer.

Authors

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Cara L. Sizemore
Partner
202.719.4192
csizemore@wiley.law

Practice Areas

Government Contracts

The interim rule expanded the scope of information that contractors will be obligated to secure using the revised security standards in NIST SP 800-171, to include not only UCTI but also "Covered Defense Information" including "critical information," "export control" information, and "[a]ny other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls."

DOD clarified that a contractor's safeguarding obligations extend not only to information received from the Government during contract performance, but also to any covered defense information that is "collected, developed, received, used, or stored by or on behalf of the contractor in support of the performance of the contract." Likewise, DOD clarified that the safeguarding obligations apply to covered defense information regardless of whether it was previously marked with a restricted distribution legend prior to receipt by the contractor.

Given the significant expansion in scope, industry expressed concern with both the immediacy of the interim rule and the lack of flexibility to implement the new NIST 800-171 requirements, many of which require corporate investment and planning to efficiently implement. Following a public meeting on December 14, 2015, DOD issued another interim rule on December 30, 2015, that provided flexibility in phasing-in the new baseline. *See* 80 Fed. Reg. 81472. The revision allowed for a two-year phase-in period for contractors to implement the adequate security requirements outlined NIST SP 800-171, and requiring contractors to implement those standards "as soon as practical, but not later than December 31, 2017." DOD was sensitive to the need "to provide immediate relief from the requirement to have NIST 800-171 security requirements implemented at the time of contract award," as contractors would otherwise be "at risk of not being able to comply with the terms of contracts that require the handling of covered defense information" upon contract award under the initial interim rule.

Notwithstanding the phase-in period, contractors must still notify DOD within 30 days after contract award "of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award," with an undertaking to implement the necessary standards later. This will enable DOD to monitor compliance trends and determine whether further revisions are warranted. Contractors will also have the flexibility to consider implementing "[a]lternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection," with written authorization by a representative of the DOD Chief Information Officer. This will provide additional flexibility for contractors that lack the organizational structure or resources needed to implement discrete requirements.

DOD's interim rules also create new obligations for contractors that plan to utilize cloud-based computing services to meet government information technology (IT) services requirements. Contractors that will fulfill DOD IT services requirements using a cloud-based solution must specify that plan in their proposals and obtain contracting officer approval. Among the requirements that DOD imposed, cloud-based service providers must:

- Obtain provisional authorization from the Defense Information Systems Agency (DISA);
- Provide access to the relevant data, contract personnel, and related facilities during any government audit, inspection, investigation, or similar activity;

- Store all government cloud-based data within the United States, unless the data is physically located on DOD premises or the contracting officer grants prior approval.

Cloud-based information services will be subject to cyber incident reporting requirements involving any cyber incidents, discovery of malicious software, spillage, or requests for access to data from third parties, including from any federal, state, or local agency. In the event of a cyber incident, contractors must preserve images of all known affected systems for at least 90 days after the submission of the cyber incident report, and provide DOD access to any information or equipment necessary for a forensic analysis.

OMB Proposed Guidance

In August 2015, the Office of Management and Budget (OMB) released proposed Guidance intended to improve cybersecurity for "controlled unclassified information" (CUI) that resides on contractor information systems. The Guidance came on the heels of the massive U.S. Office of Personnel Management (OPM) data breach earlier in the year, and appears to piggy-back on many of the developments DOD implemented in its UCTI rule. The proposed Guidance was expected to be reissued in "the Fall" as "final" Guidance, but the final Guidance remains a work in progress. Ideally, any final Guidance, as well as any rulemaking by the FAR Council to implement the Guidance, will take into consideration the same challenges and need for flexibility that DOD adopted (albeit belatedly) with its December 2015 interim rule.

In general, OMB's Guidance aligns with DOD's baseline, and will require government contractors who collect or maintain information on behalf of a federal agency to implement similar security controls, conduct security assessments, and report cyber incidents. The proposed Guidance distinguishes between systems that are "operated on behalf" of the Government including systems performing "outsourced" services and functions, versus contractor internal information services used to provide a product or service to the Government. The distinction is significant, and the consequence having a contractor system characterized as one "operated on behalf" of the Government will be potentially higher levels of data protection, reporting obligations, continuous monitoring requirements, and government audit/investigation rights:

- **Data Protection:** Systems that are operated on behalf of the Government will be required to meet the security baselines in NIST SP 800-53, with each agency determining whether its risk profile falls as the low, moderate or high-risk baseline. Systems that contain CUI will be required to meet the "moderate baseline" security controls. Contractor systems that process CUI incidental to developing a product or service will have to meet the baseline established in NIST SP 800-171.
- **Reporting Obligations:** Contractors operating systems on behalf of the Government will be required to timely report ***all*** cyber incidents, while contractors operating their own systems have to report only incidents affecting CUI.
- **Continuous Monitoring:** Contractors operating systems on behalf of the Government will have to deploy continuous monitoring software developed by the U.S. Department of Homeland Security, use other monitoring software selected by the agency, or develop proprietary software that meets minimum requirements and is approved by the agency. Contractors operating their own systems, by contrast, will have to deploy continuous monitoring software in a manner consistent with the NIST 800-171 guidance,

and will therefore have more flexibility in developing or installing monitoring software suited to their unique system requirements.

- **Security Assessments:** The Guidance calls for the Government to conduct security assessments of contractor systems, obtain third-party assessments, or rely on contractor self-assessments. The Guidance suggests that the Government may be able to obtain "access to the contractor's facilities, installations, operations, documentation, databases, IT systems, devices, and personnel used in performance of the contract" to conduct security "inspection, evaluation, investigation or audit and to preserve evidence of information security incidents." Presumably, systems operated "on behalf of" the Government would be subject to more rigorous audit and inspection rights. The Guidance also suggests that agencies develop contract clauses that would require contractors to certify the sanitization of government data at the conclusion of performance.
- **Due Diligence Database:** The Guidance requires the U.S. General Services Administration (GSA) to maintain a "business due diligence information shared service." The stated goal of the due diligence service would be to allow agencies to have access to "comprehensive information about current and prospective contractors and subcontractors" in order to assess the contractor's potential cybersecurity risk. Based on the Guidance, the database sounds like it would operate similarly to a past performance database, but the Guidance did not provide any details regarding due process that would allow contractors to review data inputs to the database or challenge incorrect information.

The language in the draft OMB Guidance is broad and primarily policy-oriented. Ultimately, the proverbial devil will be in the details of whatever rulemaking efforts come out of the final Guidance that OMB issues. In the meantime, contractors must continue to be attuned to the risk that civilian agencies may begin to make their own interim interpretations of the draft Guidance and implement a hodgepodge of new Section H contract requirements that require compliance with NIST SP 800-53 or 800-171 requirements, along with cyber incident reporting and/or certification requirements. We expect significant development in this arena to continue to play out over the next 18 months, and will continue to provide updates and analysis as they unfold.