COVINGTON

OMB Issues New Draft Cyber Guidance for Contractors

August 12, 2015

Government Contracts

On August 11, 2015, the Office of Management and Budget (OMB) issued a draft guidance memorandum intended to improve cybersecurity protections in federal acquisitions. Specifically, the proposed memorandum provides direction to federal agencies on "implementing strengthened cybersecurity protections in Federal acquisitions for products or services that generate, collect, maintain, disseminate, store, or provides access to Controlled Unclassified Information (CUI) on behalf of the Federal government." CUI is defined in a recently issued proposed FAR rule as "information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information."

Although the OMB memorandum is a laudable attempt to create uniformity across the federal government, the Guidance leaves many questions unanswered and the details of its implementation by federal agencies remains to be seen. As described below, even with this Guidance, contractors will continue to encounter inconsistent requirements for what constitutes a "cyber incident," how quickly a cyber incident must reported to the government, and what security controls are considered "adequate" for safeguarding CUI.

Scope of the Guidance

Although not entirely clear, the OMB Guidance appears to impose requirements on two types of systems: (1) those "operated on behalf of the government" where the contractor provides data processing services that the Government might otherwise perform itself but has decided to outsource; and (2) "internal contractor systems" used to provide a product or service for the government where the processing of CUI is incidental to contract performance.

Under the proposed OMB Guidance, information systems "operated on behalf of the government" will be required to meet NIST SP 800-53 and conform to the same standards as government-operated systems. "Internal contractor information systems" generally will be subject to the requirements described in NIST SP 800-171. Importantly, OMB's Guidance makes clear that the applicable NIST standards will only provide "the appropriate baseline" for security controls and, as a result, each federal agency will still be required to tailor the NIST standards to meet their own unique "risk management requirements." For example, information systems operated "on behalf of the government" for multiple users will likely require variations from the standard government processes or terms of service.

Five Areas of Guidance

The OMB Guidance states that the Federal Acquisition Regulatory Council should amend the Federal Acquisition Regulation (FAR) to include contract clauses that address, as appropriate, five cyber-related areas: (1) security controls, (2) cyber incident reporting, (3) information system security assessments, (4) information security continuous monitoring, and (5) business due diligence.

Security Controls

- For systems operated on behalf of the Government, contractor systems must meet the appropriate baseline in NIST SP 800-53, as modified by the agency to meet the agency's risk management requirements and to account for non-government customers (*i.e*, cloud service providers). For CUI in these systems, the Guidance provides that the moderate baseline for confidentiality should be applied and adjusted for any specific protection requirements required by law, regulation, or government-wide policy.
- For contractors' internal systems that are used to provide a product or service for the Government but that also contain CUI, contractors must comply with NIST SP 800-171.

Cyber Incident Reporting

- OMB's Guidance defines a "cyber incident" as "actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein." Not only is this a very broad definition, but it is also different from that contained in the DoD's rule on unclassified controlled technical information (UCTI) and from the "sensitive information incident" definition contained in the Department of Homeland Security's (DHS) Class Deviation, as noted below.
- OMB's Guidance requires agencies to include language in contracts that addresses the following minimum cyber-incident reporting requirements:
  - a definition of a "cyber incident" and the timeline for reporting;
  - language noting that properly reported cyber incidents shall not, by themselves, be interpreted as evidence that the contractor has failed to provide adequate information safeguards for CUI;
  - descriptions of the information that must be reported in each cyber incident report;
  - limiting reports to one point of contact in each agency; and
  - specific government remedies if a contractor fails to report according to the agreed upon contractual language.
- The OMB Guidance is clear that contractors only need to report a cyber incident if the incident impacts the CUI in the contractor's internal information systems. In addition to reporting to the agency's Security Operation Center (SOC), agencies must add contractual language requiring the contractor to report cyber incidents to the:
  - Contracting Officer (CO);
  - Contracting Officer Representative (COR);
  - Chief Information Security Officer (CISO); and

- Senior agency official for privacy (SAOP).

Information System Security Assessments

- The OMB Guidance requires agencies to develop an approach to assessing information systems operated by contractors. For those contractors that receive an Authority to Operate (ATO), agencies should use relevant existing ATOs as an indication of common controls and capabilities for the performance of multiple contracts. Similarly, the Guidance recognizes that contractors operating in the commercial marketplace already receive a variety of independent assessments to protect other data and that these assessments should inform an ATO process that meets NIST standards and guidelines.
- In the assessment process, the agency must require contractors to give the agency access to the contractor's "facilities, installations, operations, documentation, databases, IT systems, devices, and personnel used in performance of the contract, regardless of location." Agencies will be required to identify in the solicitation how contractors will be required to demonstrate that they meet the requirements of NIST SP 800-171. The Guidance indicates that this could range from a simple attestation of compliance to a detailed description of the system's security architecture, controls, and/or the provision of supporting test data.
- Finally, agencies will be obligated to include contract language requiring the contractor to certify, prior to contract closeout, that it has sanitized government and government-activity-related files and information.

Information Security Continuous Monitoring

- Given the increase and complexity of cyber incidents, the government has prioritized Information Security Continuous Monitoring (ISCM). NIST defines ISCM "as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions." To assist agencies in establishing ISCM capabilities quickly, the DHS has created the Continuous Diagnostics and Mitigation (CDM) program.
- For contractors operating information systems on behalf of the government, if the agency determines that providing the DHS CDM capabilities to a contractor operating information systems on behalf of the Government is not feasible, agencies must require contractors to meet or exceed the information security continuous monitoring requirements identified in M-14-03 or perform information security continuous monitoring and IT security scanning of contractor systems with tools and infrastructure of the agency's choosing.
- For contractor internal systems that contain CUI – continuous monitoring is part of the security assessment requirement in NIST SP 800-171.

Business Due Diligence

- OMB posits that cybersecurity protections in federal acquisitions can be enhanced by performing increased business due diligence to gain better visibility into how contractors "assure integrity, security, resilience, and quality in their operations." The OMB Guidance therefore requires agencies to assess the security risks posed by potential contractors.
- The approach appears similar to a past performance type review and will include assessments of predecessor firms. In the Frequently Asked Questions accompanying the Guidance, OMB noted that agencies already take performance problems of

predecessor firms and key employees into account when selecting vendors during the procurement process and this would be a similar analysis. In particular, agencies must consider whether prospective vendors have a satisfactory performance record, along with the necessary "organization, experience, accounting, technical and operational controls."

- Within 90 days of the issuance of this Guidance, the Working Group is further required to identify and make recommendations on risk indicators that should be used as a baseline for business due diligence research and analysis.

OMB's Guidance Leaves Important Questions Unanswered

As is evident from the foregoing, and the Guidance itself, OMB left several important questions unanswered, including:

- **How will different federal agencies implement OMB's Guidance in a manner that actually achieves "greater uniformity" across the federal procurement system?** Although OMB has tasked the FAR Council with developing standard solicitation and contract clauses in several key cyber-related areas, the Guidance makes clear that individual agencies will still be required to develop their own unique contract provisions and protocols for, among other things, (i) defining a "cyber incident," (ii) establishing a timeline for reporting cyber incidents to the government, (iii) specifying contractual remedies available to the government if a contractor does not comply with the agency's requirements, (iv) conducting security assessments of contractors' systems, and (v) conducting "due diligence" reviews of contractors' cybersecurity systems and capabilities.
- **How will the government reconcile existing or proposed regulations and guidance in this area?** OMB's Guidance does not attempt to reconcile existing or proposed regulations and guidance in this area, including those previously issued by the Department of Defense (DoD). For example as to safeguarding requirements, DoD imposes subsets of NIST SP 800-53 on contractors for information systems where unclassified controlled technical information (UCTI) either resides or transits. Those same contractors are likely to have CUI on their information systems and are now facing disparate guidance on what security controls are "adequate" for safeguarding government information. Similarly, the final FAR CUI rule is expected to impose additional safeguarding requirements in the form of NIST 800-171, but there is the potential for even more and potentially inconsistent safeguarding requirements for the same information systems.
- **What constitutes a cyber incident and how quickly must they be reported?** Although not explicit in the Guidance, it is clear that the government is concerned with timely reporting of incidents so that it can react more quickly and avoid future breaches like those at the Office of Personnel Management. Indeed, the OMB definition of a "cyber incident" includes not only the actual compromise of an information system, but also any incident that could have a "potentially adverse effect" on an information system. This is similar to the broad definition in DoD's UCTI rule, which includes the "possible exfiltration, manipulation, or other loss or compromise." DoD's rule requires a report within 72-hours of determining that a cyber incident affects UCTI. In contrast, DHS imposes a 1-hour reporting requirement for reporting any "known or suspected" sensitive information incidents. It is unclear how federal agencies tasked with implementing the

OMB Guidance will approach the timing requirements and varying reporting deadlines will make compliance even more problematic. At the same time, like DoD's UCTI rule, the Guidance states that a breach of internal contractor systems is only reportable where CUI is impacted. Making that determination in a "timely" manner, however, may be difficult when dealing with contractor information systems where government and commercial customer data are commingled.

- **How will "Business Due Diligence" reviews be conducted and utilized by federal agencies?** The OMB Guidance anticipates the creation of a shared database that will allow federal agencies to conduct cyber-related "due diligence" reviews of government contractors. This proposed system appears to be similar to the one used by agencies to conduct past performance reviews, but the Guidance does not provide detail on how this information will be used by agencies for acquisition purposes. In addition, the government anticipates that, within the next 90 days, it will produce "risk indicators" that can be used by agencies to make a baseline determination regarding, among other things, how a particular contractor assures information integrity and security. It remains to be seen, however, how such risk indicators will be used by federal agencies.

Comments are Due on September 10, 2015

- OMB is accepting comments for 30 days. Feedback can be submitted by visiting policy.cio.gov and following the posted instructions.
- Following the public feedback period, OMB will analyze all submitted feedback and revise the policy as necessary. The final guidance will be released Fall 2015.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Government Contracts practice group:

Susan Cassidy	+1 202 662 5348	scassidy@cov.com
Alex Sarria	+1 202 662 5426	asarria@cov.com