Bloomberg BNA

Federal Contracts Report™

Cybersecurity

View From RJO: OMB's New Guidance on Using Acquisition Methods to Improve Cybersecurity

BY ROBERT S. METZGER

The federal government relies upon private contractors and their supply chain. Increasingly, supply chain security has come under examination. The government has an important interest to protect sensitive but unclassified federal information in the hands of its private contractors, and to assure the integrity and availability of both the information and the information systems contractors employ to host, transmit or use this data. By Executive Order 13636, at § 8 (e), dated February 2013, President Obama directed key federal agencies to recommend how to incorporate security standards into acquisition planning and contract administration. On January 23, 2014, these agencies issued a report, ''Improving Cyber Security and Resilience through Acquisition.'' Among the suggested reforms was that the federal government institute a federal acquisition cyber risk management strategy.

Over recent months, agencies have acted to improve cyber security in the federal supply chain using acquisition authority. On May 8, 2015, the National Archives and Records Administration (NARA) issued a proposed rule on ''Controlled Unclassified Information.'' 80 Fed. Reg. 26501-26511. In June 2015, NIST released Special Publication (SP) 800–171, ''Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.'' http://www.nist.gov/manuscript-publication-search.cfm?pub_id=918804. NARA's CUI rule, when final, will inform agencies and contractors on what categories of federal information receive cyber safeguards and dissemination controls. NIST SP 800–171, developed in conjunction with the NARA, articulates the cyber security ''requirements'' for commercial companies to use to protect CUI.[1]

These actions, collectively, identify information to be protected and articulate the basis for controls to apply to that information. Missing from the equation, however, are the means to impose these controls through solicitation requirements and contract terms and conditions.

On August 11, 2015, the Office of Management and Budget (OMB) released draft guidance on ''Improving Cybersecurity Protections in Federal Acquisitions.'' https://policy.cio.gov/. OMB employed an interactive platform, GitHub, to collect public feedback on the draft guidance, and comments are due by September 10,

Rogers Joseph O'Donnell PC is a boutique law firm that specialized in public contracts for more than 33 years. Robert S Metzger is a shareholder and heads the firm's Washington office. This article presents his individual views and should not be attributed to any client of RJO or a to any organization with which it is or may be affiliated.

[1] For relevant background, see my previous article, ''*BNA Insights:* Cybersecurity and Acquisition Practices – New Initiatives to Protect Federal Information of Civilian Agencies,'' 103 FCR 625, Jun. 9, 2015.

 ISSN 0014-9063

2015. OMB anticipates release of the final guidance in Fall 2015. Agencies already are imposing new cyber measures in pending acquisitions – even as the OMB initiative continues.

OMB's action follows by about two months the revelation that a cyber breach of the Office of Personnel Management (OPM) exposed 4 million records to hackers. Subsequently, it has become known that as many as 21 million records of persons who applied for security clearance also were compromised. On June 15, OMB ordered a 30 – day ''CyberSprint'' to secure agency networks. The OPM breach involved a ''federal information system.'' Whether any federal contractor in fact bears responsibility for this breach is unclear. But the shock of so large a breach involving the personal records of so many people and of such sensitivity is driving OMB and agencies to improve cyber protection both for ''federal information systems'' (operated by the government itself or by contractors ''on behalf of'' the government) as well as ''nonfederal information systems'' (operated by contractors for their internal purposes) where federal controlled unclassified information (CUI) is hosted, used or transmitted.

OMB intends to monitor and measure agency compliance once the guidance is final. OMB will review compliance of ''contract activities,'' whether agencies are using ''security assessments'' and adherence to NIST SP 800–171. The guidance instructs agencies to continuously review contract activities to ensure that acquisitions include contract clauses to address five subject areas.

■ *Applicable Security Controls*. Systems that are operated ''on behalf of the government,'' must meet NIST SP 800-53, while CUI on ''contractor's internal systems'' are subject to the new NIST SP 800–171. Agencies are specifically instructed to require contractors to meet the requirements of NIST SP 800-171, rather than NIST 800-53, where contractors use their ''internal information systems will process CUI incidental to developing a product or service for the agency.'' This provides *some* assurance to private companies with CUI that they will not be obligated to adopt the demanding mechanics of NIST SP 800–53 as are required for federal information systems. Use of the word ''incidental,'' however, raises the prospect that individual agencies, should they characterize use of their information as *more* than ''incidental,'' will demand instead compliance with NIST SP 800–53. For a company with strong, existing safeguards, even if built around different methodologies, this would be expensive, disruptive and unnecessary.

■ *Cyber Incident Reporting*. Neither the NARA CUI proposed rule nor NIST SP 800–171 provide specific guidance on cyber incident reporting. The OMB guidance assigns to each agency the authority to determine reporting requirements. At a minimum, agencies are to include contractual language to define what constitutes a reportable cyber incident, to establish a timeline for reporting to the agency, and to identify the types of information required in an incident report. OMB states that the fact of a report shall not, by itself, be interpreted as evidence that a contractor has failed to provide adequate information safeguards. But OMB also directs agencies to include specific government remedies if a contractor fails to report as required. OMB also encourages ''timely and meaningful'' information sharing, but provides no structure for reporting and no assurance that contractors may make such reports without risk of third-party liability. Nor does OMB resolve uncertainties as to notification of individuals whose records may be affected by a cyber event. It says only that the contractor and agency should ''work together closely'' to investigate, identify affected individuals, quickly respond and ''take other appropriate actions.'' Considering the importance of personal privacy interests at risk, if CUI is exposed, the final guidance should incorporate further instructions and advance planning requirements. Implementation will be contract–specific, as notification requirements and appropriate remedial measures will depend upon the nature of information compromised and whether personal privacy interests are affected.

■ *Information System Security Assessments*. Neither the proposed CUI rule nor NIST SP 800-171 provided defined mechanisms for federal agencies to assess contractor system security. It appeared that scrutiny would be ''event-driven,'' coming after an incident. The guidance takes a different approach. OMB would include measures to evaluate contractor systems, but the draft raises as many questions as it answers. The guidance suggests use of FIPS–199 to assess the impact level of data that resides on a contractors system, but it is not clear how the impact level will affect either the assessment or required controls. The guidance allows agencies to accept independent third-party verification, but it is not clear how this will occur, to what standard, or who will do it or when. Present in the OMB guidance is the invocation to agencies to ''identify in the contract solicitation'' how they expect the contractor to demonstrate that it meets the requirements of NIST SP 800–171. The guidance also allows that demonstration ''can range'' from simple to more complex, but little is present to help contractors anticipate future demands. Contractors will be concerned that they will be held to expensive security assessments without a known assessment process framework or clearly established ''target states'' for compliance. Also unresolved is how the government will address the status quo as thousands of contractors now operate information systems with CUI but do not have and have never previously been required to obtain federal authority to operate.

■ *Information Security Continuous Monitoring*. Again in apparent reflection of painful recent experience, the guidance states that agencies ''may elect'' to perform continuous monitoring and IT security scanning of contractor systems. Specifically, the OMB guidance recognizes a new DHS Continuous Diagnostics and Mitigation (CDM) program which OMB seemingly expects agencies to use for monitoring. As an alternative, agencies to assure that contractor systems satisfy monitoring requirements identified by OMB Memorandum M-14-03 or are to perform monitoring and scanning ''with tools and infrastructure of its [the agency's] choosing.'' The particulars of this new surveillance requirement are not well-defined, will be intrusive and may not be necessary beyond ''federal information systems'' that are subject to NIST SP 800-53. One can expect strong industry resistance. Where a contractor is subject to SP 800-171, and safeguards have been suitably tailored for the contract and the nature of information at risk, the government is relying upon the contractor's system and should trust contractor-directed moni-

  FCR ISSN 0014-9063

toring, demanding federal monitoring only in exceptional and justified situations.

■ *Business Due Diligence*. Also included in OMB's guidance is a reference to GSA's initiative to access open source data to improve ''business due diligence'' in order to make available to federal purchasers more sources of data considered relevant to supplier risk. *Request for Information* (RFI) BizDueDil-RFI-001, Dec. 12, 2014, *available at* https://www.fbo.gov/utils/view?id=934b5b8cb16e52b2f184369aeb65b107. The OMB guidance includes specific instructions on how agencies should employ business due diligence research in anticipation of a ''shared service'' that GSA shall create. Such information is relevant to supply chain risk, broadly understood. But inclusion of the business due diligence initiative with this guidance on cybersecurity measures is nonetheless problematic. There is no direct connection to the primary objectives of assuring the confidentiality of CUI at private companies. As concerns the GSA RFI, industry has raised significant concerns about the accuracy of information to be collected and how it will employed. It will take time to develop the relevant methodology and to demonstrate the value of the information in acquisition decisions. GSA's business due diligence initiative should be decoupled from the remainder of the effort to achieve better cybersecurity through acquisition methods. The business due diligence project focuses upon suppliers rather than information assurance or the security of information systems.

The OMB guidance focuses upon agencies but it also informs companies of what they can expect as the agencies move to impose requirements on contractors to improve their cyber security and respond to new reporting and notification obligations. Especially as applied to contractor (''non-federal'') information systems, when agencies act these new acquisition measures there will be important consequences. There will be substantial cost consequences. Implementation may cause delay and disruption to the ability of government agencies to achieve their purposes and missions. There will be difficult implementation challenges for contractors and their supply chain.

Given the pervasive and insidious cyber threat, and painfully demonstrated consequences when security fails, there are many good reasons to accept these costs and delays as necessary in today's threat environment. Not all security objectives can be achieved for all programs and purposes concurrently, or affordably. Choices must be made. This emphasizes the importance of a risk-based approach, at OMB and within each agency and department, to apply new acquisition methods and controls first of those contracts where the risks to mission or to privacy interests of individuals are greatest. At the same time, Congress as well as the agencies and departments will have to step up to provide funding to pay the additional costs. And agencies must take care not to make federal cyber burdens so onerous that they become a barrier separating the federal government from sources of commercial innovation and competition.