Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# What The OMB Cybersecurity Proposal Does And Doesn't Do

*Law360, New York (August 19, 2015, 10:59 AM ET) --*

Evan D. Wolff

On Aug. 11, the U.S. Office of Management and Budget published the proposed guidance "Improving Cybersecurity Protections in Federal Acquisitions," and is seeking feedback through Sept. 10. Ostensibly, the proposal aims to strengthen cybersecurity in federal procurement and thus highlights the critical role that the private sector plays in protecting the federal government's sensitive information.

The proposed guidance comes as part of the Obama administration's ongoing efforts to better educate the nation about, and secure it from, cyberthreats. Early last year, the National Institute of Standards and Technology, in response to an executive order, released the first iteration of its cybersecurity framework to help private sector entities, particularly those involved in critical infrastructure, better address cyberrisks. Just one year later, the president issued another executive order calling for enhanced cyberinformation sharing between the public and private sectors, including through the use of information sharing and analysis organizations.

The contracting community is no stranger to cybersecurity requirements. The Federal Information Security Management Act (FISMA) has been on the books since 2002 and was revised just last year — reflecting Congress' willingness to impose data security requirements on private federal contractors in a way that it has thus far been reluctant to do for the private sector as a whole. We have also seen a slew of cyber-specific contracting regulations in the past few years. The details of many are still pending — with one exception. The Defense Federal Acquisition Regulation Supplement Safeguarding Clause has applied to U.S. Department of Defense contracts for almost two years now. It is not surprising, then, that the proposed OMB guidance appears to take an approach similar to the DFARS requirements but with applicability to all federal contractors.

Final since Nov. 18, 2013, the DFARS Clause 252.204-7012, Safeguarding of Unclassified Controlled Technical Information, imposes two sets of requirements on defense contractors who handle unclassified but controlled technical information (UCTI).

First, covered defense contractors must implement "adequate security" on their information systems housing UCTI. They can achieve "adequate security" by, at a minimum, adopting 51 specific security

controls listed in NIST Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, a complex and evolving federal standard currently undergoing a fifth revision. Covered defense contractors may adopt other standards, such as ISO 27002, but they must persuade the DOD that their alternative controls provide protection that is at least equivalent to that provided by the NIST controls.

Notably, achieving "adequate security" is not a check-the-box exercise. Covered defense contractors must go beyond the specified controls when known risks demand additional security. Meeting the Safeguarding Clause's "adequate security" requirement thus entails a dynamic and considered response to a shifting threat environment.

Second, covered defense contractors must report defined cyberincidents to the DOD within 72 hours of their discovery. The Safeguarding Clause defines a "cyberincident" as "actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein." Examples of "reportable" cyberincidents include the "possible exfiltration, manipulation, or other loss or compromise of any [UCTI] resident on or transiting through" a contractor's — or its subcontractor's — unclassified information systems, and also "any other activities" that allow unauthorized access to a contractor's unclassified information systems on which UCTI is resident or transiting. Somewhat confusingly, not all "reportable" cyberincidents need be reported. Covered defense contractors need only report cyberincidents that "affect" UCTI, though neither the clause nor related guidance explains what constitutes an "affect."

While the Safeguarding Clause is certainly at the vanguard of cyber regulations, it has not been resoundingly embraced. Contracting officers and defense contractors alike have struggled with what the clause actually requires and how to feasibly meet those requirements. These difficulties have led to mixed implementation. In February, however, the DOD released a formal memorandum reiterating how vital UCTI is to national security, and then chastising its components for not adequately incorporating the clause into DOD contracts and solicitations, despite the fact that they are obliged to do so. The message was clear: The Safeguarding Clause is not optional.

The proposed OMB guidance, on the other hand, is just that — guidance. It is not final. Nor is it a rule, at least for now, as it calls for the amendment of the Federal Acquisition Regulation and actions by the General Services Administration and others to incorporate its recommendations. But the practical impact cannot be overstated. It foreshadows the likely inevitability that all federal contractors will eventually grapple with the challenges that defense contractors already face under the Safeguarding Clause.

If released as drafted, the proposed guidance will have a broad reach and significant impact on the entire federal acquisition process. To start, it applies to all federal contractors, not just those working under the DOD. It also applies to any form of controlled but unclassified information (CUI), going beyond the unclassified controlled technical information regulated by the Safeguarding Clause. And finally, it applies to two types of information systems: those a contractor operates "on behalf of the government," i.e., systems that an agency could operate itself but has nevertheless outsourced, and "internal information systems" that a contractor uses to process CUI incidental to developing a product or service for the government. It also prescribes more than just security and incident reporting requirements. It also addresses security assessments, continuous monitoring, and agency due diligence.

All contractors should pay particular attention to the five key areas identified in the proposed guidance:

***1. Security Controls***

For contractor systems operated on behalf of the government, the proposed guidance provides that NIST SP 800-53 — only parts of which are required under the Safeguarding Clause — would serve as the baseline for mandatory information security and privacy controls. Contractors whose internal information systems incidentally process CUI must meet the requirements of the recently published NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. The proposed guidance directs agencies to adjust and tailor the applicable NIST standard to meet, among other things, agency risk management requirements.

***2. Cyberincident Reporting***

Regarding internal contractor systems, the proposed guidance limits a contractor's reporting obligations to cyberincidents that impact CUI in their system. Although the proposed guidance defines "cyberincident" to mean "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," each agency may craft its own definition.

Agencies must include contract clauses establishing an incident reporting timeline (which must account for the sensitivity of the stored information); the types of information to be reported; and specific remedies for failing to report incidents as required. Paralleling the Safeguarding Clause, all contracts must also make clear that a "properly reported cyberincident," shall not, by itself, be a basis for concluding that the contractor failed to adequately protect CUI.

***3. Information System Security Assessments***

Under the proposed guidance, contractors operating on behalf of government agencies will be subject to initial and ongoing compliance reviews and must have an agency-issued authority to operate their information system, in accordance with NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems. This guide imposes a complex and multistep review and certification process and, like SP 800-53, the standard is continually evolving.

The proposed guidance directs agencies to "consider" certain factors when assessing a contractor's information systems, including the Federal Information Processing Standard-199, which agencies use to assess the impact level of the relevant data and thus to determine whether an independent security assessment is required.

Similar to requirements already imposed through the Safeguarding Clause, contractors must provide government access to resources used in performance of the contract, to the extent required "to conduct an inspection, evaluation, investigation or audit and to preserve evidence of information security incidents." In addition, agencies must include contract language requiring contractors to certify, prior to contract closeout, the sanitization of "government and government-activity-related files and information."

***4. Information Security Continuous Monitoring***

The proposed guidance requires continuous monitoring of all information systems containing CUI, whether internal or operated on behalf of the government. Agencies must either use contract clauses requiring compliance with Federal Information Security Continuous Monitoring (ISCM) requirements

and participation in the U.S. Department of Homeland Security-run Continuous Diagnostics and Mitigation program, or clauses ensuring that the information system otherwise meets or exceeds the ISCM requirements established by OMB Memorandum M-14-03. Contracts using the latter approach must also include a clause permitting agencies to use tools and infrastructure "of [their] choosing" to continuously monitor and scan contractor systems.

***5. Business Due Diligence***

The proposed guidance also formalizes the role of "robust business due diligence" in agency risk management by requiring agency program officers to work with their chief information officers to identify and prioritize planned acquisitions and contracts that could benefit from research providing "comprehensive information about current and prospective contractors and subcontractors" and highlighting "potential security and other risks." In addition, the proposed guidance requires the GSA to make business due diligence information and research tools available to agencies for use throughout the acquisition, sustainment, and disposal lifecycles.

Lastly, within 90 days of publishing the finalized guidance, an interagency working group must identify and make recommendations regarding risk indicators that will form a baseline for the GSA's business due diligence research and analysis, among other components.

To the extent that the proposed guidance is intended to improve cybersecurity for information systems containing CUI, it is not clear that, as written, it will provide the clarity and practical guidance sought by federal agencies and contractors alike. The current administration may be missing an opportunity to significantly improve and standardize cybersecurity practices.

First, the proposed guidance perpetuates information security challenges that agencies and contractors currently face. It identifies information security requirements and specific considerations, but ultimately leaves agencies with the discretion to interpret and apply those requirements and considerations on a contract-specific basis, based on a complex interplay of FISMA requirements, OMB memoranda, NIST guidance, and agency-specific and contract-specific issues. As has become apparent in recent months, federal agencies already have difficulty interpreting and applying existing information security requirements in a predictable and consistent manner.

Second, it is unclear whether the OMB considered alternatives to the current FISMA-based cybersecurity compliance regime. FISMA requires significant agency resources for reporting and analysis. And it has been criticized for not efficiently improving cybersecurity practices, even for those agencies that comply — or almost comply — with its requirements. The current momentum to improve federal cybersecurity practices should not reinforce prior, less-effective practices. A practical, efficient and effective approach to information security, based on collaboration between the public and private sector, seems preferable. Given the short time frame for comments on the proposed guidance, such a solution seems unlikely to emerge.

Finally, even accepting the proposed guidance's overall approach, there are many areas in which different agencies and their contractors will continue to use inconsistent information security requirements. For example, the proposed guidance allows different agencies to impose different security controls to protect the same type of information; establish different reporting requirements for cyberincidents; and apply different risk management analyses when assessing information system security. In addition, the deference to agency discretion, and differences of opinion about how that discretion should be exercised, means that federal agencies and the contractors working with them will

continue to face heightened cybersecurity scrutiny from Congress, the OMB, the Government Accountability Office and inspectors general about information security practices.

As important as it is to identify key issues underlying information security, which the proposed guidance does in its five principles, it is equally important to provide sufficient detail about those principles, whether in the FAR or other materials, to guide agencies and contractors in meaningful ways. We cannot yet tell whether the proposed guidance does so. Whether its implementation will significantly improve federal cybersecurity thus remains equally unclear.

—By Kate M. Growley, Peter B. Miller, Maida Oringher Lerner and Evan D. Wolff, Crowell & Moring LLP

*Kate Growley is an associate in the Privacy & Cybersecurity Group of Crowell & Moring's Washington, D.C. office. Peter Miller is senior counsel in the firm's Washington office and former chief privacy officer at the Federal Trade Commission. Maida Lerner is senior counsel in the firm's Washington office. Evan Wolff is a partner in the firm's Washington office, co-chairman of the firm's privacy and cybersecurity group, and former adviser to the senior leadership at the Department of Homeland Security.*

*The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.*

---

All Content © 2003-2015, Portfolio Media, Inc.