wiley

ALERT

# Office of Management and Budget Releases Proposed Cybersecurity Guidelines for Government Contractors

August 14, 2015

The Office of Management and Budget (OMB) released proposed guidance designed to take "major steps" to improve cybersecurity in Federal acquisitions. The proposed guidance, available **here**, requires that government contractors who collect or maintain information on behalf of a federal agency implement additional cybersecurity practices, including certain security controls, incident reporting, security assessments, and system monitoring.

The proposed guidance is different for systems that are "operated on behalf" of the government and a contractor's internal system that is used to provide a product or service to the government. Under the proposed guidance, systems that are operated on behalf of the government and use Controlled Unclassified Information (CUI) will be required to meet the "moderate baseline" security controls established by National Institute of Standards and Technology (NIST) SP 800-53. A contractor's internal system, however, will not have to meet all of the requirements of NIST SP 800-53. Rather, contractors who collect or maintain CUI on their own internal system will have to comply with NIST SP 800-171, which governs handling CUI.

The proposed guidance also requires reporting cyber incidents that affect a system that is operated on behalf of the government. Under the proposed guidance, contractors would have to report cyber incidents on their own internal systems if the cyber incident affected CUI. In addition, the proposed guidance would require that contractors undergo system security assessments. Depending on the nature of government information that is on the system, the security assessments may be as simple as a statement of compliance by the

## Authors


Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law


## Practice Areas

Government Contracts
Privacy, Cyber & Data Governance

contractor or as onerous as a detailed description and analysis of the system's security controls.

Under the proposed guidance, contractors that maintain or collect information on behalf of a federal agency would also be required to use software capable of continuously monitoring their network for cybersecurity vulnerabilities. The proposed guidelines did not mandate the use of any specific monitoring software. Rather, contractors may be required to use the Continuous Diagnostics and Mitigation (CDM) program created by the Department of Homeland Security, use their own monitoring software if it meets certain standards, or use monitoring software selected by the contracting agency.

Lastly, the proposed guidance tasks the General Services Administration (GSA) with maintaining 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.

Comments on the proposed guidance are due by September 10, 2015. OMB stated it intends to publish the final guidance in the fall of 2015.