WINSTON & STRAWN LLP

BLOG

New Cybersecurity Rules for Government Contractors Take Shape

OCTOBER 28, 2015

In the past several months, new cybersecurity requirements for government contractors that are intended to establish a more uniform approach to safeguarding controlled unclassified information (CUI) have slowly taken shape. In 2010, Executive Order 13556, "Controlled Unclassified Information," set in motion a process intended to do away with the patchwork of agency-specific policies and requirements for safeguarding CUI and substitute a more uniform approach applicable to federal government contractors. In the past several months, the release of draft OMB Guidance, the publication of the final version of NIST SP 800-171, and the issuance of a proposed rule by the National Archives and Record Administration (NARA) have provided key insights into the likely requirements of the final rules that will be published in 2016. While these recent publications promise a more uniform government-wide approach to CUI, they also include many significant requirements that may necessitate changes to a contractor's information security architecture and practices. To read more about this issue, see our recent briefing.

Tip: Government contractors that handle CUI should examine the requirements of the OMB Draft Guidance, the draft NARA rule, and NIST SP 800-171 now and compare these requirements to their current information security architecture, practices, and policies.

1 Min Read

Related Locations

Washington, DC

Related Capabilities

Privacy & Data Security

Government Contracts & Grants

Related Regions

North America

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.