THE BUZZ
REDGRAVE LLP
ON INFORMATION MATTERS

JANUARY 17, 2012

# Federal Government Unveils New Security Standards for Cloud-Based Service Providers

On Wednesday, officials from the General Services Administration (GSA), Department of Homeland Security (DHS), and Department of Defense (DOD) unveiled the Federal Risk and Authorization Management Program, or "FedRAMP," an initiative aimed at establishing security requirements and authorization procedures for cloud service providers.

The authorization process will rely heavily on private security firms, who will serve as "cloud IT security auditors" or "Third Party Assessment Organizations" (3PAO's) for cloud service providers seeking to do business with the federal government. These auditors, once certified by FedRAMP, will ensure that providers meet the designated security requirements.

The requirements were first established by the National Institute for Science and Technology (NIST) for federal information systems, before being modified for use with cloud services by FedRAMP. The security controls are designed for low- and moderate-impact systems (designations reflecting the sensitivity of government systems) with 116 controls for low-impact cloud systems and 297 controls for moderate-impact systems.

Businesses that host both public and private cloud services may be interested in the list of controls, which is available at the FedRAMP website,[1] as a comprehensive, state-of-the-art description of practices designed to secure cloud-based networks. With the help of NIST, FedRAMP has added 46 new, cloud-specific controls, including: backup systems for certain cloud elements, role-based access controls for enforcing assigned privileges and permissions and access privileges specific to different types of media. NIST Special Publication 800-53 (Revision 3) explains the terminology, original controls and further "enhancements," and is available at the NIST website.[2]

The public will have a chance to comment on, and suggest changes to, the list of controls and the overall process, which has yet to be finalized. The agencies in charge of FedRAMP anticipate that the initial list of certified 3PAO's will be released "on or about March 31, 2012." At that point, cloud service providers can begin seeking authorization to host and process government data.

The January 11, 2012, FedRAMP presentation is available at: http://www.actgov.org/knowledgebank/documentsandpresentations/Documents/Program%20Events/GSA%20Federal%20Risk%20and%20Authorization%20Management%20Program%20Security%20Controls%20Briefing,%201-11-12.pdf

---

[1] http://www.gsa.gov/graphics/staffoffices/FedRAMP_Security_Controls_Final.zip.
[2] http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf.

*Contact Us: For further information or if you have any questions regarding this Alert, please contact your Redgrave LLP attorney or Managing Partner Victoria Redgrave at (202) 681-2599 or vredgrave@redgravellp.com.*