Cloud Security With FedRAMP

Peter Silva, 2012-10-01

Want to provide Cloud services to the federal government? Then you'll have to adhere to almost 170 security controls under the recently announced Federal Risk and Authorization Management Program. The program, set to go live in June, is designed to analyze/audit cloud computing providers for federal government agencies, expedite security clearances for cloud providers and foster the adoption of cloud computing by the Federal government. FedRAMP is meant to provide a baseline for low to moderate risk systems and is based on the NIST cyber-security Special Publication 800-53 Revision 3. FedRAMP provides an overall checklist for handling risks associated with Web services that would have a limited, or serious impact on government operations if disrupted. Cloud providers must implement these security controls to be authorized to provide cloud services to federal agencies. The government will forbid federal agencies from using a cloud service provider unless the vendor can prove that a FedRAMP-accredited third-party organization has verified and validated the security controls. Once approved, the cloud vendor would not need to be 're-evaluated' by every government entity that might be interested in their solution. There may be instances where additional controls are added by agencies to address specific needs.

Independent, third-party auditors are tasked with testing each product/solution for compliance which is intended to save agencies from doing their own risk management assessment. Details of the auditing process are expected early next month but includes a System Security Plan that clarifies how the requirements of each security control will be met within a cloud computing environment. Within the plan, each control must detail the solutions being deployed such as devices, documents and processes; the responsibilities of providers and government customer to implement the plan; the timing of implementation; and how solution satisfies controls. A Security Assessment Plan details how each control implementation will be assessed and tested to ensure it meets the requirements and the Security Assessment Report explains the issues, findings, and recommendations from the security control assessments detailed in the security assessment plan. Ultimately, each provider must establish means of preventing unauthorized users from hacking the cloud service.

The regulations allow the contractor to determine which elements of the cloud must be backed up and how frequently. Three backups are required, one available online. All government information stored on a provider's servers must be encrypted. When the data is in transit, providers must use a "hardened or alarmed carrier protective distribution system," which detects intrusions, if not using encryption. Since cloud services may span many geographic areas with various people in the mix, providers must develop measures to guard their operations against supply chain threats. Also, vendors must disclose all the services they outsource and obtain the board's approval to contract out services in the future.

More details of the FedRAMP program will be available from the General Services Administration by February 8th, but they have already started accepting applications for third party assessment vendors.

ps

Resources:

- Contractors dealt blanket cloud security specs
- FedRAMP includes 168 security controls
- New FedRAMP standards first step to secure cloud computing
- GSA to tighten oversight of conflict-of-interest rules for FedRAMP
- What does finalized FedRAMP plan mean for industry?
- New FedRAMP standards first step to secure cloud computing
- GSA reopens cloud email RFQ
- NIST, GSA setting up cloud validation process
- FedRAMP Security Controls Unveiled
- FedRAMP security requirements benchmark IT reform
- FedRAMP baseline controls released
- Federal officials launch FedRAMP
- Audio: Steven VanRoekel announces FedRAMP
- NIST: Cloud providers should adopt portability standards
- Cloud security breach inevitable as businesses underestimate security due diligence

Technorati Tags: F5, federal government, integration, cloud computing, Pete Silva, security, business, fedramp, technology, nist, cloud, compliance, regulations, web, internet

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com