

Contractors dealt blanket cloud security specs

Department of Homeland Security Homeland Security CIO Richard Spires said the process "will evaluate IT services offered by vendors on behalf of federal agencies." The White House is speeding ahead on a program to expedite security clearances for cloud products, having just notified contractors of about 170 specific protections soon to be required.

The [security controls](#), released Friday, are intended to prepare agencies and vendors for the Federal Risk and Authorization Management Program, or FedRAMP, that is slated to go live in June.

The publication is a one-size-fits-all checklist for handling risks associated with Web services that would have "low," meaning limited, or "moderate," meaning serious, impact on government operations if disrupted. By following this list, supporters say, the government will be able to inspect a product once, assured that it will meet any agency's security needs. And providers won't have to waste time being approved by every single agency interested in their products.

But the bar has to be set high enough to satisfy picky agencies, to achieve an expected 30 percent to 40 percent savings in testing and procurement costs, some security auditors say. Agencies can't be tempted to customize the list.

The spreadsheet of specifications builds off existing security controls for federal information technology systems in [National Institute of Standards and Technology Special Publication 800-53](#). Within those items, there are about 70 related, cloud-specific stipulations that cover smartphone access, software upgrades, backups and other vulnerability issues.

Under the FedRAMP approach, independent auditors are to test each product for compliance. Friday's notice announces that the General Services Administration, which is responsible for managing the program, is to spell out how the auditing routine will work by Feb. 8.

According to the specifications, each provider must establish means of preventing unauthorized users from hacking cloud services on employees' mobile devices. A "joint authorization board" consisting of security experts from the Homeland Security Department, Pentagon and GSA then will vet the proposed safeguards.

Typically, with physical software and systems, every enhancement requires another evaluation to check whether the new feature has introduced more vulnerabilities. But some cloud providers, which may update their software weekly, contend that such retesting would defeat the whole purpose of FedRAMP.

The regulations leave it up to the company and the board to agree on the types of changes that will trigger an additional assessment. Since those substantial modifications would affect multiple agencies, the rules state the contractor must publicize them on a central website, such as a service status page.

The regulations allow the contractor to decide on which elements of the cloud must be backed up and how frequently. Three backups are required, one of which will be available online.

All government information stored on a provider's servers must be encrypted, according to the guidelines. When the data is in transit, providers must use a "hardened or alarmed carrier protective distribution system," which detects intrusions, if not using encryption.

Any cloud service inherently touches many geographic areas and comes into contact with many people, including programmers and hardware developers. The situation makes it difficult to monitor supply chains for malicious activity -- such as the installation of "backdoors" that can remotely knock out systems or steal information. So, providers must develop measures to guard their operations against supply chain threats, the publication states.

In addition, vendors must disclose all the services they outsource and obtain the board's approval to contract out services in the future.

"FedRAMP's unified risk management process will evaluate IT services offered by vendors on behalf of federal agencies, saving agencies from conducting their own risk management programs," DHS Chief Information Officer Richard Spires wrote in a [blog post](#). "This baseline serves all federal agencies and [cloud service providers], to which additional controls may be added by agencies to meet specific requirements."

Some businesses planning to apply for FedRAMP auditing positions have argued that the standards should be stringent enough to prevent agencies from saddling themselves and contractors with additional evaluations.

"As a service provider I would rather have a more rigorous audit that I had to go through once, as opposed to 10 different less rigorous audits," Chris Wysopal, co-founder of computer security firm Veracode, said last week. "That would save everybody time."
