FAST FUTURE

ACCELERATING INNOVATION

(https://fastfuture.org/)

FedRAMP cloud cybersecurity guidelines: Is your organization ready? Should it be?

Edit (https://fastfuture.org/wp-admin/post.php?post=502719&action=edit)

January 11, 2023

(https://fastfuture.org/wp-content/uploads/2023/01/cybersecurity-concept.jpg)

Image: BeeBright/Shutterstock

Companies working with the federal government are likely aware of the need to upgrade to align with new FedRAMP (https://www.gsa.gov/technology/government-it-initiatives/fedramp) guidelines, signed into law by President Joe Biden on Dec. 23, 2022. The new guidelines (https://www.fedramp.gov/) require that commercial cloud or software providers that host, process or transmit federal data must be FedRAMP authorized.

OK, great. So what does that mean for your company? Should you be working toward this standard of cybersecurity?

We chatted with Tom McAndrew, CEO of Denver-based Coalfire (https://www.coalfire.com/), a cybersecurity company that works with 70% of all cloud service providers that work with the federal government. Coalfire helps companies become FedRAMP ready.

“If something can move to the cloud and be leveraged by many agencies, then it should move,” McAndrew said. “This is related to the government’s desire to ‘assess once, leverage many times’ as well as save money and standardize cybersecurity across the government.”

McAndrew said the measure will be significant: “The federal government is sending a bold message to agencies and commercial businesses that FedRAMP is here to stay,” he said in a press release (https://www.prnewswire.com/news-releases/coalfire-releases-guidance-as-president-joe-biden-signs-fedramp-authorization-act-into-law-301709758.html). “The passage of the FedRAMP Authorization Act will stimulate innovation and drive agencies to seek ‘cloud-first’ technology solutions, making for a safer, more security-conscious country.”

From FISMA (Federal Information Security Modernization Act (https://csrc.nist.gov/projects/risk-management/fisma-background)) in 2002 (updated in 2014 (https://www.cisa.gov/federal-information-security-modernization-act)) to the original FedRAMP in 2011

(https://www.fismacenter.com/fedrampmemo.pdf), the FedRAMP Authorization Act accelerates secure cloud adoption for federal agencies. The new FedRAMP reform is expected to spread into state and local governments and have a major impact on security standards across the commercial economy.

While many organizations have continued to upgrade security, the threat landscape has moved faster and many high-profile attacks have caused governments and businesses to be very concerned about potential breaches from hackers, ransomware and even nation-state attacks. Outdated security systems are still in place, making businesses and governments vulnerable.

“By formalizing the concepts of ‘reciprocity’ and ‘presumption of adequacy,’ agencies can more easily certify vendors,” McAndrew said. “This provides government access to a wider range of security solutions and services, and commercial providers easier access to multiple agencies.”

(https://fastfuture.org/wp-content/uploads/2023/01/Tom-McAndrew.jpg)

Image: Courtesy of Coalfire

Tom McAndrew, CEO of Coalfire

Not all companies need to upgrade, McAndrew said, but it’s definitely worth considering if you do business with government agencies.

Companies often support other solutions that are under contract with the federal government, McAndrew said. These B2B relationships may pull solutions into scope for a FedRAMP authorization. “Each company should assess the risks and benefits of achieving ATO in context with their customer and supply-chain relationships. A FedRAMP ATO represents an acceptance of risk on the part of a government agency, and therefore requires a government sponsor,” he said.

For those companies that do secure FedRAMP ATO, there are other benefits outside of just securing new federal revenue streams, including:

- As the “gold standard” in cloud security, FedRAMP authorization establishes brand trust and confidence in the security of an offering beyond just federal agencies.
- With the passage of the FedRAMP Authorization Act (FRAA) contained in the FY23 National Defense Authorization Act, commercial cloud and software providers will now have easier access to multiple agencies across the federal marketplace – making the business case for pursuing FedRAMP even better.

“On the other hand, some companies think that getting FedRAMP compliant will create business for them,“ McAndrew said. “‘Build it and they will come’ is not a good strategy. To be successful, organizations must first understand how the government buys and their cycles. There are unique things like Lowest Price Technically Acceptable (LPTA), sole source awards, contract vehicles, set asides, and other government-specific processes that must be understood to take a compliant solution to market.”

McAndrew said cloud migration is no longer a “nice to have” for federal agencies. And he said he thinks FedRAMP should go further for more security.

"To make the biggest impact for FedRAMP and the newly passed FRAA, there is more that needs to be done to help drive adoption of ATO'd solutions – unfortunately, far too many agencies still do not leverage FedRAMP-authorized solutions. The program needs 'teeth,' and there will eventually come mandates and consequences for agencies and contractors that fail to comply," he said. "No longer can anyone afford to fall behind the adoption curve. I believe there would be greater adoption if there were teeth in mandating the adoption. There are still far too many agencies buying expensive, custom solutions, and continuing to receive funding even though they are not meeting the requirements."

While there may be growing pains involved in adopting FedRAMP security tools and practices, in the long run, it will make companies and organizations more secure and help ensure smoother transitions for government contracting agencies.

McAndrew said FedRAMP is "solving one of the hardest problems in government: establishing a common cybersecurity baseline of services. Under these guidelines, CSPs have been able to establish a win/win ecosystem for both government and commercial customers, and are delivering a level of scalability, flexibility and productive engagement never before experienced between public and private sectors."

Posted in ITSR Newsletters (https://fastfuture.org/category/newsletters/itsr-newsletter/), Newsletters (https://fastfuture.org/category/newsletters/), Stories (https://fastfuture.org/category/stories/)