Federalist memorandum

Transformation Technology Services
General Services Administration

From

Eddie A Tejeda
Director, Federalist
General Services Administration

Subject

Compliance of Federalist system for hosting static websites

To

Interested Parties

Date

January 15, 2019

Federalist serves our fellow federal employees by expertly managing the backend and compliance work to launch and manage a website, allowing them to focus their expertise on their content.

This memo discusses Federalist's compliance.

Basic information about Federalist

Federalist serves our fellow federal employees by expertly managing the backend and compliance work to launch and manage websites, allowing our partners to focus their expertise on their content. Federalist does this by loading in partner content, using it to build static web pages, then deploying the pages to highly scalable GSA cloud infrastructure. Federalist also makes it easy to preview and approve site changes, unlocking the potential of partner agency small teams to quickly launch attractive, secure, and accessible public websites.

Federalist memorandum

Transformation Technology Services
General Services Administration

Authority to operate

Federalist carries a GSA ATO at the Low Impact Level that is valid until March 5, 2021. Federalist leverages two Authorities to Operate (ATOs) in addition to its own. First, Federalist is deployed on Amazon Web Services (AWS) GovCloud infrastructure, which has been FedRAMP JAB Authorized at the High Impact Level[1] since June 21, 2016. Second, Federalist extensively leverages services of cloud.gov, which has been FedRAMP JAB Authorized at the Moderate Impact Level[2] since February 2, 2017. Federalist's specific implementation of cloud.gov's services to host static sites carries a GSA Agency ATO at the Low Impact Level as of February 7, 2017. GSA's ATO is at low impact because Federalist's partner agencies have not requested Moderate Impact and we want to control costs.

How Federalist builds work

Federalist loads, builds, and deploys static files. Federalist builds and deploys site content by using an ephemeral, isolated container for each individual site build. That container has three processes: First, it loads a specific site's data from a code repository. Second, another container process may run static site build engines such as Jekyll or Hugo that generate HTML pages and associated web content using site data. Alternatively, partner agencies may generate the content before it is loaded into Federalist, skipping this step. Third, a final container process takes the resulting files (either created by the build tool or pre-built) and moves them onto a cloud.gov S3 service. The container is then destroyed until another build is ready.

In the event that an adversary gains controls of a code repository deployed on Federalist using a partner's credentials while breaking their mandatory two-factor

[1] FedRAMP†Package†ID†F1603047866
[2] FedRAMP†Package†ID†F1607067912

authentication, this configuration prevents the adversary from harming anything beyond the initially compromised content. The general public does not interact with the Federalist build system, but instead only with the content after deployment on S3.

How Federalist hosting works

Federalist hosts sites using cloud.gov deployments of Amazon services like S3 and CloudFront. Site data is stored on S3 and cannot be changed by any Federalist user; S3 credentials to modify site data are restricted to three cloud.gov users with the Federalist administrator permissions. To access the credentials which are not stored on any local machine, these users must always authenticate into cloud.gov using cloud.gov authentication and the GSA SecureAuth system, which requires multi-factor authentication.

The public accesses Federalist web content using two intermediaries that provide different forms of security. First, a cloud.gov service deploys an Amazon CloudFront Content Delivery Network (CDN) Distribution for the specific site. This allows cloud.gov to own HTTPS certificate generation and renewal for all Federalist sites at no additional cost to the partner agency. It also provides protection against distributed denial of service attacks. Second, the CloudFront distribution loads content from S3 via a NGINX proxy service that adds various required headers for user security, including a prohibition against access outside of the HTTPS protocol[3] and an X-Frame-Options header to block clickjacking attacks.[4] These two tools connect a web address like 18f.gsa.gov to the source S3 files and work together to meet GSA security requirements.

Federalist accounts

Federalist accounts are only granted at the request of verified government Federalist partners. Federalist accounts also grant no access to cloud.gov or AWS.

[3] https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
[4] https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Instead, these accounts allow partner agencies to configure some aspects of how Federalist loads and deploys their own content to Federalist's hosting system, which is secured by the cloud.gov. Access to Federalist, by itself, does not grant access to any specific site data, which remains under the exclusive control of the Federalist partner agency and out of the control of Federalist administrators. Federalist partners must have access to modify site data on GitHub in order to deploy a site on Federalist or adjust Federalist settings.

Vulnerability disclosure policy and bug bounty

Federalist is covered by the GSA TTS vulnerability disclosure policy. It was the first ever federal civilian application to be placed under a public bug bounty where private sector researchers are financially compensated for discovering and reporting security issues or weaknesses. One of the researchers invited to the bug bounty, Evgeniy Yakovchuk, said:

> "I must admit, that the Federalist team did very great work on securing their application...this project is one of the best that take care of security, from my experience on HackerOne. It's a great pleasure for me to work with you. Keep up your great work!"

Appendix

Discussion of static sites security and compliance advantages

Federalist sites are static files hosted in a read-only storage service that does not accept inputs, such as comments or form submissions. It only provides HTML pages or related static assets such as CSS files as required by browsers. HTML pages on Federalist cannot be changed or modified in any way without the credentials to update the storage service. Protection of those credentials is detailed below.

This system architecture presents a very narrow attack surface. Account compromise of a Federalist user does not compromise the security of the build

system and content on S3 is highly resilient to denial of service attacks. Segmentation also reduces risk. If the Federalist build system is down for any reason, website content hosted by Federalist will remain available to the public.

FedRAMP service description by AWS GovCloud High

AWS GovCloud (US) is an AWS Region designed to allow US government agencies and customers supporting the US government to move more sensitive workloads into the cloud. In addition to complying with FedRAMP requirements, the AWS GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations. Additional information is available at https://aws.amazon.com/govcloud-us/.

The following AWS services are FedRAMP Authorized and approved by the JAB: S3, EC2, EBS, VPC, IAM, RDS(Oracle, MySQL, PostgreSQL), CloudWatch Logs, CloudTrail, Cloud Formation, Amazon Glacier, Amazon Web Services Key Management Service, Amazon Simple Workflow Service, Amazon Simple Queue Service, Amazon Simple Notification Service, Amazon DynamoDB, Amazon Elastic MapReduce, Amazon Redshift.[5]

FedRAMP Service Description by cloud.gov

cloud.gov is designed and operated by US government workers for US government work. cloud.gov reduces the barriers to rapid, incremental, compliant, secure, and scalable delivery of government services by all government agencies, leveraging best-of-breed modern practices. Cloud.gov provides a Platform-as-a-Service (PaaS) based on Cloud Foundry, enabling instant provisioning of services and environments, easy deployment of applications, and rapid scaling to match demand. cloud.gov includes tools to quickly incorporate 800-53 NIST control documentation into easily-prepared and comprehensive System Security Plans (SSPs) for evaluation by local agency information security organizations or FedRAMP, reducing the time it takes for teams to gain Authority To Operate (ATO).[6]

[5] Source: https://marketplace.fedramp.gov/
[6] Ibid.