

# Pages memorandum



**Transformation Technology Services  
General Services Administration**

From

**Lindsay Young**

Director, cloud.gov

General Services Administration

Subject

**Compliance of Pages  
system for hosting static websites**

To

**Interested Parties**

Date

**October 01, 2021**

---

Pages 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 Pages' compliance.

## **Basic information about Pages**

Pages 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. Pages does this by loading in partner content, using it to build static web pages, then deploying the pages to highly scalable GSA cloud infrastructure. Pages 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.

# Pages memorandum



Transformation Technology Services  
General Services Administration

## Authority to operate

Pages is operated by cloud.gov and is fully integrated into the cloud.gov PaaS ATO boundary. cloud.gov has been FedRAMP JAB Authorized at the Moderate Impact Level since February 2, 2017. Leveraging the cloud.gov PaaS, Pages is deployed on Amazon Web Services (AWS) GovCloud infrastructure, which has been FedRAMP JAB Authorized at the High Impact Level since June 21, 2016.

## How Pages builds work

Pages loads, builds, and deploys static files. Pages 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 Pages, 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 control of a code repository deployed on Pages using a partner's credentials while breaking their mandatory two-factor authentication, this configuration prevents the adversary from harming anything beyond the initially compromised content. The general public does not interact with the Pages build system, but instead only with the content after deployment on S3.

# Pages memorandum



Transformation Technology Services  
General Services Administration

## How Pages hosting works

Pages 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 Pages user; S3 credentials to modify site data are restricted to three cloud.gov users with the Pages 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 Pages 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 Pages 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<sup>1</sup> and an X-Frame-Options header to block [clickjacking](#) attacks.<sup>2</sup> These two tools connect a web address like [18f.gsa.gov](#) to the source [S3 files](#) and work together to meet GSA security requirements.

## Pages accounts

Pages accounts are only granted at the request of verified government Pages partners. Pages accounts also grant no access to cloud.gov or AWS. Instead, these accounts allow partner agencies to configure some aspects of how Pages loads and deploys their own content to Pages' hosting system, which is secured by the cloud.gov. Access to Pages, by itself, does not grant access to any specific site data, which remains under the exclusive control of the Pages partner agency and out of

---

<sup>1</sup> <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security>

<sup>2</sup> <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

# Pages memorandum



## Transformation Technology Services General Services Administration

the control of Pages administrators. Pages partners must have access to modify site data on GitHub in order to deploy a site on Pages or adjust Pages settings.

### **Vulnerability disclosure policy and bug bounty**

Pages 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 Pages 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**

Pages 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 Pages 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 Pages 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 Pages build system is down for any reason, website content hosted by Pages will remain available to the public.

# Pages memorandum



Transformation Technology Services  
General Services Administration

## **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.<sup>3</sup>

## **FedRAMP Service Description by cloud.gov**

[cloud.gov](https://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).<sup>4</sup>

---

<sup>3</sup> Source: <https://marketplace.fedramp.gov/>

<sup>4</sup> Ibid.